3Com WX3000 Series Unified Switches Switching Engine

Operation Manual

Manual Version: 6W100
www.3com.com

3Com Corporation
350 Campus Drive, Marlborough,
MA, USA 01752 3064



Copyright © 2009, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com’s standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

About This Manual

Organization

3Com WX3000 Series Unified Switches consists of three models: the WX3024 , the WX3010 and the WX3008. *3Com WX3000 Series Unified Switches Switching Engine Operation Manual* is organized as follows:

Part	Contents
1 CLI	Introduces the command hierarchy, command view and CLI features of the WX3000 Series Unified Switches Switching Engine.
2 Login	Introduces the ways to log into an WX3000 Series Unified Switches Switching Engine.
3 Configuration File Management	Introduces configuration file and the related configuration.
4 VLAN	Introduces VLAN-/Voice VLAN-related configuration.
5 Auto Detect	Introduces auto detect and the related configuration.
6 Voice VLAN	Introduces voice VLAN and the related configuration.
7 GVRP	Introduces GVRP and the related configuration.
8 Basic Port Configuration	Introduces basic port configuration.
9 Link Aggregation	Introduces link aggregation and the related configuration.
10 Port Isolation	Introduces port isolation and the related configuration.
11 Port Security-Port Binding	Introduces port security, port binding, and the related configuration.
12 DLDP	Introduces DLDP and the related configuration.
13 MAC Address Table Management	Introduces MAC address forwarding table management.
14 MSTP	Introduces STP and the related configuration.
15 802.1x and System Guard	Introduces 802.1x and the related configuration.
16 AAA	Introduces AAA, RADIUS, HWTACACS, EAD, and the related configurations.
17 MAC Address Authentication	Introduces centralized MAC address authentication and the related configuration.
18 IP Address and Performance	Introduces IP address and IP performance related configuration.
19 DHCP	Introduces DHCP-Snooping, DHCP Client and the related configuration.
20 ACL	Introduces ACL and the related configuration.
21 QoS-QoS Profile	Introduces QoS and the related configuration.
22 Mirroring	Introduces mirroring and the related configuration.
23 ARP	Introduces ARP and the related configuration.

Part	Contents
24 SNMP-RMON	Introduces the configuration for network management through SNMP and RMON
25 Multicast	Introduces IGMP snooping and the related configuration.
26 NTP	Introduces NTP and the related configuration.
27 SSH	Introduces SSH2.0 and the related configuration.
28 File System Management	Introduces basic configuration for file system management.
29 FTP-SFTP-TFTP	Introduces basic configuration for FTP, SFTP and TFTP, and the applications.
30 Information Center	Introduces information center configuration.
31 System Maintenance and Debugging	Introduces daily system maintenance and debugging.
32 VLAN-VPN	Introduces VLAN VPN and the related configuration.
33 HWPing	Introduces HWPing and the related configuration.
34 DNS	Introduces DNS and the related configuration.
35 Smart Link-Monitor Link	Introduces Smart Link, Monitor Link and the related configuration.
36 PoE-PoE Profile	Introduces PoE, PoE profile and the related configuration.
37 Routing Protocol	Introduces the static route, RIP, and IP route policy configurations.
38 UDP Helper	Introduces UDP Helper and the related configuration.
39 Appendix	Lists the acronyms used in this manual.

Conventions

The manual uses the following conventions:

Command conventions

Convention	Description
Boldface	The keywords of a command line are in **Boldface**.
italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected.

Convention	Description
&<1-n>	The argument(s) before the ampersand (&) sign can be entered 1 to n times.
#	A line starting with the # sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
 **Warning**	Means reader be extremely careful. Improper operation may cause bodily injury.
 **Caution**	Means reader be careful. Improper operation may cause data loss or damage to equipment.
 **Note**	Means a complementary description.

Related Documentation

In addition to this manual, each 3Com WX3000 Series Unified Switches Switching Engine documentation set includes the following:

Manual	Description
3Com WX3000 Series Unified Switches Installation Manual	It introduces the installation process, startup, hardware and software maintenance of WX3000 Series unified switches.
3Com WX3000 Series Unified Switches Switching Engine Command Manual	Elaborates on the operation commands for WX3000 series unified switches switching engines. It covers the operation commands for CLI, login, VLAN, GVRP, basic port configurations, MAC address table management, MSTP, 802.1x, AAA, ACL, QoS, SNMP, RMON, NTP, and SSH.
3Com WX3000 Series Unified Switches User Manual	Provides a guide to the operation of WX3000 series unified switches access controller engines. It covers configurations of CLI, VLAN, system maintenance and debugging, WLAN, IPv4, IPv6, port basic configurations, multicast protocols, 802.1x, AAA, SSH, ACL, QoS, description of the acronyms used throughout the manual, and a command index.

Manual	Description
3Com WX3000 Series Unified Switches Web-Based Configuration Manual	Introduces the Web-based functions of the access control engine of WX3000 series unified switches access controller engines.

Obtaining Documentation

You can access the most up-to-date 3Com product documentation on the World Wide Web at this URL: http://www.3com.com.

Table of Contents

1 CLI Configuration 1-1
Introduction to the CLI 1-1
Command Hierarchy 1-1
Switching User Levels 1-2
Setting the Level of a Command in a Specific View 1-3
CLI Views 1-4
CLI Features 1-7
Online Help 1-7
Terminal Display 1-8
Command History 1-8
Error Prompts 1-9
Command Edit 1-9

1 CLI Configuration



Note

The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Introduction to the CLI

A command line interface (CLI) is a user interface to interact with a device. Through the CLI on a device, a user can enter commands to configure the device and check output information to verify the configuration. Each device provides an easy-to-use CLI and a set of configuration commands for the convenience of the user to configure and manage.

The CLI on the devices provide the following features, and so has good manageability and operability.

- Hierarchical command protection: After users of different levels log in, they can only use commands at their own, or lower, levels. This prevents users from using unauthorized commands to configure devices.
- Online help: Users can gain online help at any time by entering a question mark (?).
- Debugging: Abundant and detailed debugging information is provided to help users diagnose and locate network problems.
- Command history function: This enables users to check the commands that they have lately executed and re-execute the commands.
- Partial matching of commands: The system will use partially matching method to search for commands. This allows users to execute a command by entering partially-spelled command keywords as long as the keywords entered can be uniquely identified by the system.

Command Hierarchy

The device uses hierarchical command protection for command lines, so as to inhibit users at lower levels from using higher-level commands to configure the device.

Based on user privilege, commands are classified into four levels:

- Visit level (level 0): Commands at this level are mainly used to diagnose network, and they cannot be saved in configuration file. For example, **ping**, **tracert** and **telnet** are level 0 commands.
- Monitor level (level 1): Commands at this level are mainly used to maintain the system and diagnose service faults, and they cannot be saved in configuration file. Such commands include **debugging** and **terminal**.
- System level (level 2): Commands at this level are mainly used to configure services. Commands concerning routing and network layers are at this level. These commands can be used to provide network services directly.

- Manage level (level 3): Commands at this level are associated with the basic operation modules and support modules of the system. These commands provide support for services. Commands concerning file system, FTP/TFTP/XModem downloading, user management, and level setting are at this level.

Users logged into the device fall into four user levels, which correspond to the four command levels respectively. Users at a specific level can only use the commands at the same level or lower levels.

By default, the Console user (a user who logs into the device through the Console port) is a level-3 user, and Telnet users are level-0 users.

Switching User Levels

After logging into the device, users can change their current user levels through a command. Note that:

- If a switching password is set for a specific user level by the **super password** command, all users must enter the password correctly when they switch from lower user levels to this level (if a wrong password is entered, they will remain at their original levels).
- If no switching password is set for a specific user level, the Console user can directly switch to the level, while the Telnet users at lower levels will fail to switch to the level (they will remain at their original levels) and the information like the following will be displayed: % Password is not set.

Setting a user level switching password

Follow these steps to set a password for use level switching:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the super password for user level switching	**super password** [**level** *level*] { **cipher** | **simple** } *password*	Required By default, the super password is not set.

Switching to a specific user level

Follow these steps to switch to a specific user level:

To do…	Use the command…	Remarks
Switch to a specified user level	**super** [*level*]	Required Execute this command in user view.

Note

- If no user level is specified in the **super password** command or the **super** command, level 3 is used by default.
- For security purpose, the password entered is not displayed when you switch to another user level. You will remain at the original user level if you have tried three times but failed to enter the correct password.

Configuration example

After a general user telnets to the device, his/her user level is 0. Now, the network administrator wants to allow general users to switch to level 3, so that they are able to configure the device.

A level 3 user sets a switching password for user level 3.

```
<device> system-view
[device] super password level 3 simple 123
```

A general user telnets to the device, and then uses the set password to switch to user level 3.

```
<device> super 3
 Password:
User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

After configuring the device, the general user switches back to user level 0.

```
<device> super 0
User privilege level is 0, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

Setting the Level of a Command in a Specific View

Setting the level of a command in a specific view

Commands fall into four levels: visit (level 0), monitor (level 1), system (level 2), and manage (level 3). By using the following command, the administrator can change the level of a command in a specific view as required.

Follow these steps to set the level of a command output description in a specific view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the level of a command in a specific view	**command-privilege level** *level* **view** *view command*	Required

Caution

- It is recommended not to change the level of a command arbitrarily, for it may cause inconvenience to maintenance and operation.
- When you change the level of a command with multiple keywords, you should input the keywords one by one in the order they appear in the command syntax. Otherwise, your configuration will not take effect.

Configuration example

The network administrator (a level 3 user) wants to change some TFTP commands (such as **tftp get**) from level 3 to level 0, so that general Telnet users (level 0 users) are able to download files through TFTP.

Change the **tftp get** command in user view (shell) from level 3 to level 0. (Originally, only level 3 users can change the level of a command.)

```
<device> system-view
[device] command-privilege level 0 view shell tftp
[device] command-privilege level 0 view shell tftp 192.168.0.1
[device] command-privilege level 0 view shell tftp 192.168.0.1 get
[device] command-privilege level 0 view shell tftp 192.168.0.1 get bootrom.btm
```

After the above configuration, general Telnet users can use the **tftp get** command to download file bootrom.btm and other files from TFTP server 192.168.0.1 and other TFTP servers.

CLI Views

CLI views are designed for different configuration tasks. They are both correlated and distinguishing. For example, once a user logs into a device successfully, the user enters user view, where the user can perform some simple operations such as checking the operation status and statistics information of the device. After executing the **system-view** command, the user enters system view, where the user can go to other views by entering corresponding commands.

Table 1-1 lists the CLI views provided by the device, operations that can be performed in different CLI views and the commands used to enter specific CLI views.

Table 1-1 CLI views

View	Available operation	Prompt example	Enter method	Quit method
User view	Display operation status and statistical information of the device	<device>	Enter user view once logging into the device.	Execute the **quit** command to log out of the device.
System view	Configure system parameters	[device]	Execute the **system-view** command in user view.	Execute the **quit** or **return** command to return to user view.

View	Available operation	Prompt example	Enter method	Quit method
Ethernet port view	Configure Ethernet port parameters	1000 Mbps Ethernet port view: [device-GigabitEthernet1/0/1]	Execute the **interface gigabitethernet** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
		10 Gigabit Ethernet port view: [device-TenGigabitEthernet1/1/1]	Execute the **interface tengigabitethernet** command in system view.	
VLAN view	Configure VLAN parameters	[device-vlan1]	Execute the **vlan** command in system view.	
VLAN interface view	Configure VLAN interface parameters	[device-Vlan-interface1]	Execute the **interface Vlan-interface** command in system view.	
Loopback interface view	Configure loopback interface parameters	[device-LoopBack0]	Execute the **interface loopback** command in system view.	
NULL interface view	Configure NULL interface parameters	[device-NULL0]	Execute the **interface null** command in system view.	
Local user view	Configure local user parameters	[device-luser-user1]	Execute the **local-user** command in system view.	
User interface view	Configure user interface parameters	[device-ui-aux0]	Execute the **user-interface aux** command in system view.	
FTP client view	Configure FTP client parameters	[ftp]	Execute the **ftp** command in user view.	
SFTP client view	Configure SFTP client parameters	sftp-client>	Execute the **sftp** command in system view.	
MST region view	Configure MST region parameters	[device-mst-region]	Execute the **stp region-configuration** command in system view.	
Cluster view	Configure cluster parameters	[device-cluster]	Execute the **cluster** command in system view.	
Public key view	Configure the RSA public key for SSH users	[device-rsa-public-key]	Execute the **rsa peer-public-key** command in system view.	Execute the **peer-public-key end** command to return to system view.
	Configure the RSA or DSA public key for SSH users	[device-peer-public-key]	Execute the **public-key peer** command in system view.	

View	Available operation	Prompt example	Enter method	Quit method
Public key editing view	Edit the RSA public key for SSH users	[device-rsa-key-code]	Execute the **public-key-code begin** command in public key view.	Execute the **public-key-code end** command to return to public key view.
	Edit the RSA or DSA public key for SSH users	[device-peer-key-code]		
Basic ACL view	Define rules for a basic ACL (with ID ranging from 2000 to 2999)	[device-acl-basic-2000]	Execute the **acl number** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Advanced ACL view	Define rules for an advanced ACL (with ID ranging from 3000 to 3999)	[device-acl-adv-3000]	Execute the **acl number** command in system view.	
Layer 2 ACL view	Define rules for an layer 2 ACL (with ID ranging from 4000 to 4999)	[device-acl-ethernetframe-4000]	Execute the **acl number** command in system view.	
QoS profile view	Define QoS profile	[device-qos-profile-a123]	Execute the **qos-profile** command in system view.	
RADIUS scheme view	Configure RADIUS scheme parameters	[device-radius-1]	Execute the **radius scheme** command in system view.	
ISP domain view	Configure ISP domain parameters	[device-isp-aaa123.net]	Execute the **domain** command in system view.	
HWPing view	Configure HWPing parameters	[device-hwping-a123-a123]	Execute the **hwping** command in system view.	
HWTACACS view	Configure HWTACACS parameters	[device-hwtacacs-a123]	Execute the **hwtacacs scheme** command in system view.	
PoE profile view	Configure PoE profile parameters	[device-poe-profile-a123]	Execute the **poe-profile** command in system view.	
Smart-link group view	Configure smart-link group parameters	[device-smlk-group1]	Execute the **smart-link group** command in system view.	
Monitor-link group view	Configure monitor-link group parameters	[device-mtlk-group1]	Execute the **monitor-link group** command in system view.	
Port-group view	Configure port-group parameters	[device-port-group-1]	Execute the **port-group** command in system view.	

View	Available operation	Prompt example	Enter method	Quit method
QinQ view	Configure QinQ parameters	[device-GigabitEthernet1/0/1-vid-20]	Execute the **vlan-vpn vid** command in Ethernet port view. The **vlan-vpn enable** command should be first executed.	Execute the **quit** command to return to Ethernet port view. Execute the **return** command to return to user view.

Note

The shortcut key combination **Ctrl+Z** is equivalent to the **return** command.

CLI Features

Online Help

When configuring the device, you can use the online help to get related help information. The CLI provides two types of online help: complete and partial.

Complete online help

1) Enter a question mark (?) in any view on your terminal to display all the commands available in the view and their brief descriptions. The following takes user view as an example.

```
<device> ?
User view commands:
  boot             Set boot option
  cd               Change current directory
  clock            Specify the system clock
  cluster          Run cluster command
  copy             Copy from one file to another
  debugging        Enable system debugging functions
  delete           Delete a file
  dir              List files on a file system
  display          Display current system information
```

<Other information is omitted>

2) Enter a command, a space, and a question mark (?).

If the question mark “?” is at a keyword position in the command, all available keywords at the position and their descriptions will be displayed on your terminal.

```
<device> clock ?
  datetime     Specify the time and date
  summer-time  Configure summer time
```

```
  timezone     Configure time zone
```

If the question mark (?) is at an argument position in the command, the description of the argument will be displayed on your terminal.

```
[device] interface vlan-interface ?
  <1-4094>  VLAN interface number
```

If only <cr> is displayed after you enter a question mark (?), it means no parameter is available at the ? position, and you can enter and execute the command directly.

```
[device] interface vlan-interface 1 ?
  <cr>
```

Partial online help

1) Enter a character/string, and then a question mark (?) next to it. All the commands beginning with the character/string will be displayed on your terminal. For example:

```
<device> p?
   ping
   pwd
```

2) Enter a command, a space, a character/string and a question mark (?) next to it. All the keywords beginning with the character/string (if available) are displayed on your terminal. For example:

```
<device> display v?
   version
   vlan
   voice
```

3) Enter the first several characters of a keyword of a command and then press **Tab**. If there is a unique keyword beginning with the characters just typed, the unique keyword is displayed in its complete form. If there are multiple keywords beginning with the characters, you can have them displayed one by one (in complete form) by pressing **Tab** repeatedly.

Terminal Display

The CLI provides the screen splitting feature to have display output suspended when the screen is full. When display output pauses, you can perform the following operations as needed (see Table 1-2).

Table 1-2 Display-related operations

Press	To
Ctrl+C	Stop the display output and execution of the command.
Any character except the space, **Enter**, the forward slash (/), plus sign (+), and minus sign (-) when the display output pauses	Stop the display output.
The space key	Go to the next page.
Enter	Go to the next line.

Command History

The CLI provides the command history function. You can use the **display history-command** command to view a specific number of latest executed commands and execute them again in a convenient way.

By default, the CLI can store up to 10 latest executed commands for each user. You can view the command history by performing the operations listed in Table 1-3.

Table 1-3 View history commands

Purpose	Operation	Remarks
Display the latest executed history commands	Execute the **display history-command** command	This command displays the command history.
Recall the previous history command	Press the up arrow key or **Ctrl+P**	This operation recalls the previous history command (if available).
Recall the next history command	Pressing the down arrow key or **Ctrl+N**	This operation recalls the next history command (if available).

Note

- Because the Windows 9x HyperTerminal explains the up and down arrow keys in a different way, the two keys are invalid when you access history commands in a Windows 9x HyperTerminal environment. However, you can use **Ctrl+P** and **Ctrl+N** instead to achieve the same purpose.
- When you enter the same command multiple times consecutively, only one history command entry is created by the command line interface.

Error Prompts

If a command passes the syntax check, it will be successfully executed; otherwise, an error message will be displayed. Table 1-4 lists the common error messages.

Table 1-4 Common error messages

Error message	Description
Unrecognized command	The command does not exist.
	The keyword does not exist.
	The parameter type is wrong.
	The parameter value is out of range.
Incomplete command	The command entered is incomplete.
Too many parameters	The parameters entered are too many.
Ambiguous command	The parameters entered are ambiguous.
Wrong parameter	A parameter entered is wrong.
found at '^' position	An error is found at the '^' position.

Command Edit

The CLI provides basic command edit functions and supports multi-line editing. The maximum number of characters a command can contain is 254. Table 1-5 lists the CLI edit operations.

Table 1-5 Edit operations

Press…	To…
A common key	Insert the corresponding character at the cursor position and move the cursor one character to the right if the command is shorter than 254 characters.
Backspace key	Delete the character on the left of the cursor and move the cursor one character to the left.
Left arrow key or **Ctrl+B**	Move the cursor one character to the left.
Right arrow key or **Ctrl+F**	Move the cursor one character to the right.
Up arrow key or **Ctrl+P** Down arrow key or **Ctrl+N**	Display history commands.
Tab	Use the partial online help. That is, when you input an incomplete keyword and press **Tab**, if the input parameter uniquely identifies a complete keyword, the system substitutes the complete keyword for the input parameter; if more than one keywords match the input parameter, you can display them one by one (in complete form) by pressing **Tab** repeatedly; if no keyword matches the input parameter, the system displays your original input on a new line without any change.

Table of Contents

1 Logging In to the Switching Engine 1-1

Logging In to the Switching Engine 1-1

Introduction to the User Interface 1-1

Supported User Interfaces 1-1

User Interface Index 1-2

Common User Interface Configuration 1-2

2 Logging In Through OAP 2-1

OAP Overview 2-1

Logging In to the Switching Engine Through OAP 2-1

Configuring the Management IP Address of the OAP Software System 2-1

Configuring the Management IP Address of the OAP Software System on the Switching Engine 2-2

Configuring the Management IP Address of the OAP Software System of the Access Control Engine 2-2

Resetting the OAP Software System 2-3

3 Logging In Through Telnet 3-1

Introduction 3-1

Common Configuration 3-1

Telnet Configurations for Different Authentication Modes 3-2

Telnet Configuration with Authentication Mode Being None 3-3

Configuration Procedure 3-3

Configuration Example 3-4

Telnet Configuration with Authentication Mode Being Password 3-5

Configuration Procedure 3-5

Configuration Example 3-6

Telnet Configuration with Authentication Mode Being Scheme 3-7

Configuration Procedure 3-7

Configuration Example 3-10

Telnetting to the Switching Engine 3-11

Telnetting to the Switching Engine from a Terminal 3-11

Telnetting to the Switching Engine from the Access Control Engine 3-13

4 Logging In from the Web-Based Network Management System 4-1

Introduction 4-1

Setting Up a Web Configuration Environment 4-2

Configuring the Login Banner 4-3

Configuration Procedure 4-3

Configuration Example 4-4

Enabling/Disabling the WEB Server 4-5

5 Logging In from NMS 5-1

Introduction 5-1

Connection Establishment Using NMS 5-1

6 Configuring Source IP Address for Telnet Service Packets 6-1

Overview 6-1

Configuring Source IP Address for Telnet Service Packets ····· 6-1
Displaying Source IP Address Configuration ····· 6-2

7 User Control ····· 7-1
Introduction ····· 7-1
Controlling Telnet Users ····· 7-1
Prerequisites ····· 7-1
Controlling Telnet Users by Source IP Addresses ····· 7-1
Controlling Telnet Users by Source and Destination IP Addresses ····· 7-2
Controlling Telnet Users by Source MAC Addresses ····· 7-3
Configuration Example ····· 7-3
Controlling Network Management Users by Source IP Addresses ····· 7-4
Prerequisites ····· 7-4
Controlling Network Management Users by Source IP Addresses ····· 7-4
Configuration Example ····· 7-5
Controlling Web Users by Source IP Address ····· 7-5
Prerequisites ····· 7-6
Controlling Web Users by Source IP Addresses ····· 7-6
Disconnecting a Web User by Force ····· 7-6
Configuration Example ····· 7-6

1 Logging In to the Switching Engine

Note

The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Logging In to the Switching Engine

You can log in to the switching engine of the device in one of the following ways:

- Logging in through OAP
- Logging in locally or remotely through an Ethernet port by means of Telnet or SSH
- Logging in to the Web-based network management system
- Logging in through NMS (network management station)

Introduction to the User Interface

Supported User Interfaces

Note

The auxiliary (AUX) port and the console port of the device are the same port (referred to as console port in the following part). You will be in the AUX user interface if you log in through this port.

The device supports two types of user interfaces: AUX and VTY.

- AUX user interface: A view when you log in through the console port.
- Virtual type terminal (VTY) user interface: A view when you log in through VTY. VTY port is a logical terminal line used when you access the device by means of Telnet or SSH.

Table 1-1 Description on user interface

User interface	Applicable user	Port used	Description
AUX	Users logging in through the console port	Console port	Each device can accommodate one AUX user.
VTY	Telnet users and SSH users	Ethernet port	Each device can accommodate up to five VTY users.

User Interface Index

Two kinds of user interface index exist: absolute user interface index and relative user interface index.

1) The absolute user interface indexes are as follows:

- The absolute AUX user interfaces is numbered 0.
- VTY user interface indexes follow AUX user interface indexes. The first absolute VTY user interface is numbered 1, the second is 2, and so on.

2) A relative user interface index can be obtained by appending a number to the identifier of a user interface type. It is generated by user interface type. The relative user interface indexes are as follows:

- AUX user interfaces is numbered 0.
- VTY user interfaces are numbered VTY0, VTY1, and so on.

Common User Interface Configuration

Follow these steps to configure common user interface:

To do…	Use the command…	Remarks
Lock the current user interface	**lock**	Optional Execute this command in user view. A user interface is not locked by default.
Specify to send messages to all user interfaces/a specified user interface	**send** { **all** | *number* | *type number* }	Optional Execute this command in user view.
Free a user interface	**free user-interface** [*type*] *number*	Optional Execute this command in user view.
Enter system view	**system-view**	—
Set the banner	**header** [**incoming** | **legal** | **login** | **shell**] *text*	Optional By default, no banner is configured.
Set a system name for the switching engine	**sysname** *string*	Optional By default, the system name is **device.**
Enable copyright information displaying	**copyright-info enable**	Optional By default, copyright displaying is enabled. That is, the copy right information is displayed on the terminal after a user logs in successfully.
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	—

To do…	Use the command…	Remarks
Display the information about the current user interface/all user interfaces	**display users** [**all**]	Optional You can execute the **display** command in any view.
Display the physical attributes and configuration of the current/a specified user interface	**display user-interface** [*type number* | *number*]	
Display the information about the current web users	**display web users**	

2 Logging In Through OAP

OAP Overview

As an open software and hardware system, Open Application Architecture (OAA) provides a set of complete standard software and hardware interfaces. The third party vendors can develop products with special functions. These products can be compatible with each other as long as they conform to the OAA interface standards. Therefore the functions of single network product can be expanded and the users can get more benefits.

Open Application Platform (OAP) is a physical platform developed based on OAA. It can be an independent network device, or a board or program used as an extended part of a device. An OAP runs an independent operating system. You can load software such as security and voice in the operating system as needed.

Logging In to the Switching Engine Through OAP

You can log in to the access control engine through the console port on the device and perform the following configurations on the access control engine. Then, you can log in to the switching engine.

1) Execute the **oap connect slot** 0 command in user view of the access control engine to log in to the switching engine.

```
<device> oap connect slot 0
Connected to OAP!
```

2) Press Enter to enter user view of the switching engine.

```
<device_LSW>
```

Note

- To distinguish between the access control engine and the switching engine, the name of the switching engine is changed to **device_LSW** here. In fact, the default name of the switching engine is **device**.
- You can press **Ctrl+K** to return to the command line interface of the access control engine.

Configuring the Management IP Address of the OAP Software System

In the OAA system of the device, the access control engine and the switching engine integrate together and function as one device. For the snmp UDP Domain-based network management station (NMS), however, the access control engine and the switching engine are independent SNMP agents. Physically, two agents are on the same managed object; while logically, they belong to two different systems, and they manage their own MIB objects on the access control engine and the switching engine separately.

Therefore, when you use the NMS to manage the access control engine and the switching engine on the same interface, you must first obtain the management IP addresses of the two SNMP agents and obtain the link relationship between them, and then you can access the two agents. By default, the management IP address of an OAP module is not configured.

Caution

Before configuring the management IP address of the OAP software system, you must configure the same IP address at the engine side where the OAP software system resides; otherwise, the NMS cannot access the OAP software system by using the configured management IP address.

Follow these steps to configure the management IP address of the OAP software system:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the management IP address of an OAP module	**oap management-ip** *ip-address* **slot** *0*	Required Not configured by default.

Configuring the Management IP Address of the OAP Software System on the Switching Engine

1) Configure the management IP address of the OAP software system on the switching engine side.

```
<device_LSW> system-view
[device_LSW] interface vlan-interface 1
[device_LSW-Vlan-interface1] ip address 192.168.0.2 24
```

Press **Ctrl+K** to return to the command line operating interface of the access control engine.

2) Configure the management IP address of the SNMP agent on the access control engine.

```
<device> system-view
[device] oap management-ip 192.168.0.2 slot 0
```

Configuring the Management IP Address of the OAP Software System of the Access Control Engine

1) Configure the management IP address of the OAP software system on the access control engine side.

```
<device> system-view
[device] interface Vlan-interface 1
[device-Vlan-interface1] ip address 192.168.0.1 24
```

2) Log in to the switching engine, and configure the management IP address of the SNMP agent on the switching engine.

```
<device> oap connect slot 0
Connected to OAP!
<device_LSW> system-view
[device_LSW] oap management-ip 192.168.0.1 slot 0
```

Resetting the OAP Software System

If the operating system works abnormally or is under other anomalies, you can reset the OAP software system.

Follow these steps to reset the OAP software system:

To do…	Use the command…	Remarks
Reset the OAP software system	**oap reboot slot** *0*	Required Available in user view

Caution

The reset operation may cause data loss and service interruption. Therefore, before resetting the OAP software system, you need to save the data on the operating system to avoid service interruption and hardware data loss.

3 Logging In Through Telnet

Introduction

The device supports Telnet. You can manage and maintain the switching engine remotely by Telnetting to the switching engine.

To log in to the switching engine through Telnet, the corresponding configuration is required on both the switching engine and the Telnet terminal.

You can also log in to the switching engine through SSH. SSH is a secure shell added to Telnet. Refer to the *SSH Operation* for related information.

Table 3-1 Requirements for Telnetting to the switching engine

Item	Requirement
Switching engine	The IP address is configured for the VLAN of the switching engine, and the route between the switching engine and the Telnet terminal is reachable. (Refer to the *IP Address and Performance Operation* and *Routing Protocol* parts for more.)
	The authentication mode and other settings are configured. Refer to Table 3-2 and Table 3-3.
Telnet terminal	Telnet is running.
	The IP address of the VLAN of the switching engine is available.

Common Configuration

Table 3-2 lists the common Telnet configuration.

Table 3-2 Common Telnet configuration

Configuration		Description
VTY user interface configuration	Configure the command level available to users logging in to the VTY user interface	Optional By default, commands of level 0 are available to users logging in to a VTY user interface.
	Configure the protocols the user interface supports	Optional By default, Telnet and SSH protocol are supported.
	Set the commands to be executed automatically after a user log in to the user interface successfully	Optional By default, no command is executed automatically after a user logs into the VTY user interface.

Configuration		Description
VTY terminal configuration	Make terminal services available	Optional By default, terminal services are available in all user interfaces
	Set the maximum number of lines the screen can contain	Optional By default, the screen can contain up to 24 lines.
	Set history command buffer size	Optional By default, the history command buffer can contain up to 10 commands.
	Set the timeout time of a user interface	Optional The default timeout time is 10 minutes.

Telnet Configurations for Different Authentication Modes

Table 3-3 lists Telnet configurations for different authentication modes.

Table 3-3 Telnet configurations for different authentication modes

Authentication mode	Telnet configuration		Description
None	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 3-2.
Password	Configure the password	Configure the password for local authentication	Required
	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 3-2.
Scheme	Specify to perform local authentication or remote RADIUS authentication	AAA configuration specifies whether to perform local authentication or RADIUS authentication	Optional Local authentication is performed by default. Refer to the AAA part for more.
	Configure user name and password	Configure user names and passwords for local/RADIUS users	Required • The user name and password of a local user are configured on the switching engine. • The user name and password of a remote user are configured on the RADIUS server. Refer to user manual of RADIUS server for more.
	Manage VTY users	Set service type for VTY users	Required
	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 3-2.

Note

To improve security and prevent attacks to the unused Sockets, TCP 23 and TCP 22, ports for Telnet and SSH services respectively, will be enabled or disabled after corresponding configurations.

- If the authentication mode is **none**, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is **password**, and the corresponding password has been set, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is **scheme**, there are three scenarios: when the supported protocol is specified as **telnet**, TCP 23 will be enabled; when the supported protocol is specified as **ssh**, TCP 22 will be enabled; when the supported protocol is specified as **all**, both the TCP 23 and TCP 22 port will be enabled.

Telnet Configuration with Authentication Mode Being None

Configuration Procedure

Follow these steps to perform Telnet configuration with the authentication mode being none:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter one or more VTY user interface views	**user-interface vty** *first-number* [*last-number*]	—
Configure not to authenticate users logging in to VTY user interfaces	**authentication-mode none**	Required By default, VTY users are authenticated after logging in.
Configure the command level available to users logging in to VTY user interface	**user privilege level** *level*	Optional By default, commands of level 0 are available to users logging in to VTY user interfaces.
Configure the protocols to be supported by the VTY user interface	**protocol inbound** { **all** | **ssh** | **telnet** }	Optional By default, both Telnet protocol and SSH protocol are supported.
Set the commands to be executed automatically after a user login to the user interface successfully	**auto-execute command** *text*	Optional By default, no command is executed automatically after a user logs in to the VTY user interface.
Make terminal services available	**shell**	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.

To do…	Use the command…	Remarks
Set the history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time of the VTY user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that if you configure not to authenticate the users, the command level available to users logging in to the switching engine depends on the **user privilege level** *level* command

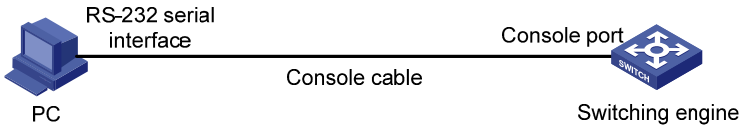
Configuration Example

Network requirements

As shown in Figure 3-1, assume current user logs in using the **oap connect slot** 0 command, and the user level is set to the manage level (level 3). Perform the following configurations for users logging in through VTY 0 using Telnet.

- Do not authenticate the users.
- Commands of level 2 are available to the users.
- Telnet protocol is supported.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

Figure 3-1 Network diagram for Telnet configuration (with the authentication mode being none)



Configuration procedure

Enter system view.

```
<device> system-view
```

Enter VTY 0 user interface view.

```
[device] user-interface vty 0
```

Configure not to authenticate Telnet users logging in through VTY 0.

```
[device-ui-vty0] authentication-mode none
```

Specify commands of level 2 are available to users logging in through VTY 0.

```
[device-ui-vty0] user privilege level 2
```

Configure Telnet protocol is supported.

```
[device-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[device-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[device-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[device-ui-vty0] idle-timeout 6
```

Telnet Configuration with Authentication Mode Being Password

Configuration Procedure

Follow these steps to perform Telnet configuration with the authentication mode being password:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter one or more VTY user interface views	**user-interface vty** *first-number* [*last-number*]	—
Configure to authenticate users logging in to VTY user interfaces using the local password	**authentication-mode password**	Required
Set the local password	**set authentication password** { **cipher** | **simple** } *password*	Required
Configure the command level available to users logging in to the user interface	**user privilege level** *level*	Optional By default, commands of level 0 are available to users logging in to VTY user interface.
Configure the protocol to be supported by the user interface	**protocol inbound** { **all** | **ssh** | **telnet** }	Optional By default, both Telnet protocol and SSH protocol are supported.
Set the commands to be executed automatically after a user login to the user interface successfully	**auto-execute command** *text*	Optional By default, no command is executed automatically after a user logs into the VTY user interface.
Make terminal services available	**shell**	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.

To do…	Use the command…	Remarks
Set the history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time of the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that when the authentication mode is password, the command level available to users logging in to the user interface is determined by the **user privilege level** *level* command.

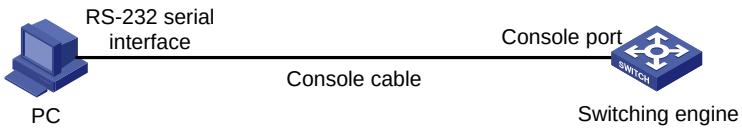
Configuration Example

Network requirements

As shown in Figure 3-2, assume current user logs in using the **oap connect slot** 0 command, and the user level is set to the manage level (level 3). Perform the following configurations for users logging in to VTY 0 using Telnet.

- Authenticate users using the local password.
- Set the local password to 123456 (in plain text).
- Commands of level 2 are available to the users.
- Telnet protocol is supported.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

Figure 3-2 Network diagram for Telnet configuration (with the authentication mode being password)



Configuration procedure

Enter system view.

```
<device> system-view
```

Enter VTY 0 user interface view.

```
[device] user-interface vty 0
```

Configure to authenticate users logging in to VTY 0 using the password.

```
[device-ui-vty0] authentication-mode password
```

Set the local password to 123456 (in plain text).

```
[device-ui-vty0] set authentication password simple 123456
```

Specify commands of level 2 are available to users logging in to VTY 0.

```
[device-ui-vty0] user privilege level 2
```

Configure Telnet protocol is supported.

```
[device-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[device-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[device-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[device-ui-vty0] idle-timeout 6
```

Telnet Configuration with Authentication Mode Being Scheme

Configuration Procedure

Follow these steps to perform Telnet configuration with the authentication mode being scheme:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Configure the authentication scheme	Enter the default ISP domain view	**domain** domain-name	Optional By default, the local AAA scheme is applied. If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well. If you specify to apply an existing scheme by providing the *radius-scheme-name* argument, you need to perform the following configuration as well: • Perform AAA and RADIUS configuration on the switching engine. (Refer to the AAA part for more.) • Configure the user name and password accordingly on the AAA server. (Refer to the user manual of the AAA server.)
	Configure the AAA scheme to be applied to the domain	**scheme** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] }	
	Quit to system view	**quit**	
Create a local user and enter local user view		**local-user** *user-name*	No local user exists by default.
Set the authentication password for the local user		**password** { **simple** | **cipher** } *password*	Required
Specify the service type for VTY users		**service-type telnet** [**level** *level*]	Required
Quit to system view		**quit**	—

To do…	Use the command…	Remarks
Enter one or more VTY user interface views	**user-interface vty** *first-number* [*last-number*]	—
Configure to authenticate users locally or remotely	**authentication-mode scheme** [**command-authorization**]	Required The specified AAA scheme determines whether to authenticate users locally or remotely. Users are authenticated locally by default.
Configure the command level available to users logging in to the user interface	**user privilege level** *level*	Optional By default, commands of level 0 are available to users logging in to the VTY user interfaces.
Configure the supported protocol	**protocol inbound** { **all** | **ssh** | **telnet** }	Optional Both Telnet protocol and SSH protocol are supported by default.
Set the commands to be executed automatically after a user login to the user interface successfully	**auto-execute command** *text*	Optional By default, no command is executed automatically after a user logs into the VTY user interface.
Make terminal services available	**shell**	Optional Terminal services are available in all use interfaces by default.
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time for the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that if you configure to authenticate the users in the scheme mode, the command level available to the users logging in to the switching engine depends on the **user privilege level** *level* command and the **service-type** { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }* [**level** *level*] } command, as listed in Table 3-4.

Table 3-4 Determine the command level when users logging in to the switching engine are authenticated in the scheme mode

Scenario			Command level
Authentication mode	**User type**	**Command**	
authentication-mode scheme [command-authorization]	VTY users that are AAA/RADIUS authenticated or locally authenticated	The **user privilege level** *level* command is not executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is not executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command
		The **user privilege level** *level* command is executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command
	VTY users that are authenticated in the RSA mode of SSH	The **user privilege level** *level* command is not executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is not executed, and the **service-type** command specifies the available command level.	
		The **user privilege level** *level* command is executed, and the **service-type** command does not specify the available command level.	Determined by the **user privilege level** *level* command
		The **user privilege level** *level* command is executed, and the **service-type** command specifies the available command level.	
	VTY users that are authenticated in the password mode of SSH	The **user privilege level** *level* command is not executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is not executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command
		The **user privilege level** *level* command is executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command

Note

Refer to *AAA Operation* and *SSH Operation* of this manual for information about AAA, RADIUS, and SSH.

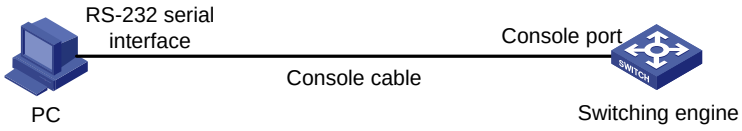
Configuration Example

Network requirements

As shown in Figure 3-3, assume a current user logs in using the **oap connect slot 0** command and the user level is set to the manage level (level 3). Perform the following configurations for users logging in to VTY 0 using Telnet.

- Configure the local user name as **guest**.
- Set the authentication password of the local user to 123456 (in plain text).
- Set the service type of VTY users to Telnet and the command level to 2.
- Configure to authenticate users logging in to VTY 0 in scheme mode.
- Only Telnet protocol is supported in VTY 0.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

Figure 3-3 Network diagram for Telnet configuration (with the authentication mode being scheme)



Configuration procedure

Enter system view.

```
<device> system-view
```

Create a local user named **guest** and enter local user view.

```
[device] local-user guest
```

Set the authentication password of the local user to 123456 (in plain text).

```
[device-luser-guest] password simple 123456
```

Set the service type to Telnet, Specify commands of level 2 are available to users logging in to VTY 0.

```
[device-luser-guest] service-type telnet level 2
[device-luser-guest] quit
```

Enter VTY 0 user interface view.

```
[device] user-interface vty 0
```

Configure to authenticate users logging in to VTY 0 in the scheme mode.

```
[device-ui-vty0] authentication-mode scheme
```

Configure Telnet protocol is supported.

```
[device-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[device-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[device-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[device-ui-vty0] idle-timeout 6
```

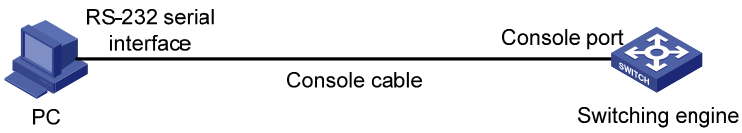
Telnetting to the Switching Engine

Telnetting to the Switching Engine from a Terminal

1) Assign an IP address to VLAN-interface 1 of the access control engine of the device (VLAN 1 is the default VLAN of the access control engine).

- Connect the serial port of your PC/terminal to the console port of the device, as shown in Figure 3-4.

Figure 3-4 Diagram for establishing connection to a console port



- Launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 95/Windows 98/Windows NT/Windows 2000/Windows XP) on the PC terminal, with the baud rate set to 9,600 bps, data bits set to 8, parity check set to none, and flow control set to none.
- Power on the device and press **Enter** as prompted. The prompt (such as <device>) appears, as shown in the following figure.

Figure 3-5 The terminal window

```
.....................................................................
.....................................................................
.....................................................
Done!
The ANP application file is self-decompressing.....................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................
Done!
System application is starting...

User interface aux0 is available.



Press ENTER to get started.
<device>
#Apr 26 12:04:08:66 2000 device SHELL/4/LOGIN:
 Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1<hh3cLogIn>: login from Console
%Apr 26 12:04:08:75 2000 device SHELL/4/LOGIN: Console login from aux0
<device>
```

- Perform the following operations in the terminal window to assign IP address 202.38.160.90/24 to VLAN–interface 1 of the access control engine.

```
<device> system-view
[device] interface Vlan-interface 1
[device-Vlan-interface1] ip address 202.38.160.90 255.255.255.0
```

- Log in to the switching engine of the device using the **oap connect slot** 0 command.

```
<device>oap connect slot 0
Connected to OAP!
```

- Configure the IP address of VLAN-interface 1 of the switching engine of the device as 202.38.160.92/24.

```
<device_LSW> system-view
[device_LSW] interface Vlan-interface 1
[device_LSW-Vlan-interface1] ip address 202.38.160.92 255.255.255.0
```

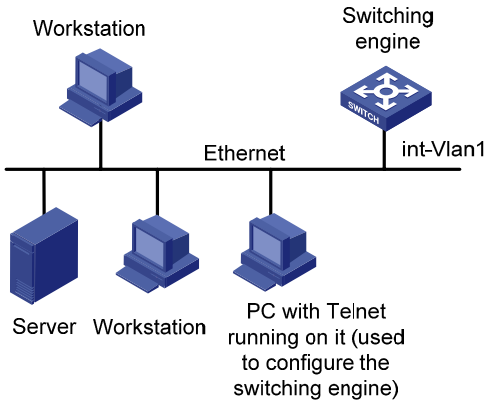
Note

To distinguish between the access control engine and the switching engine, the name of the switching engine is changed to **device_LSW** here. In fact, the default name of the switching engine is device.

---

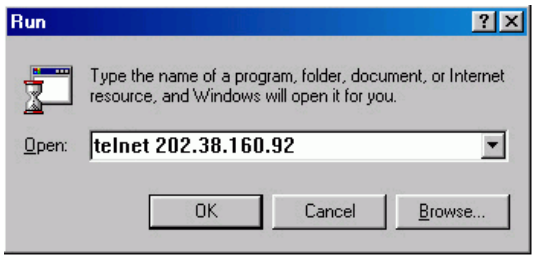
2) Perform Telnet-related configuration on the switching engine. For details, refer to Telnet Configuration with Authentication Mode Being None, Telnet Configuration with Authentication Mode Being Password, and Telnet Configuration with Authentication Mode Being Scheme.
3) Connect your PC/terminal and the switching engine to an Ethernet, as shown in Figure 3-6. Make sure the port through which the switching engine is connected to the Ethernet belongs to VLAN 1 and the route between your PC and VLAN-interface 1 is reachable.

Figure 3-6 Network diagram for Telnet connection establishment



4) Launch Telnet on your PC, with the IP address of VLAN–interface 1 of the switching engine as the parameter, as shown in Figure 3-7.

Figure 3-7 Launch Telnet



5) If the password authentication mode is specified, enter the password when the Telnet window displays “Login authentication” and prompts for login password. The CLI prompt (such as <System_LSW>) appears if the password is correct. If all VTY user interfaces of the switching engine are in use, you will fail to establish the connection and see the message “All user interfaces are used, please try later!” The switching engine of the device can accommodate up to five Telnet connections at same time.
6) After successfully Telnetting to the switching engine, you can configure the switching engine or display the information about the switching engine by executing corresponding commands. You can also type ? at any time for help. Refer to the relevant parts in this manual for the information about the commands.

Note

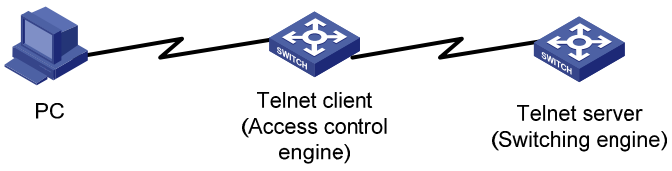
- A Telnet connection is terminated if you delete or modify the IP address of the VLAN interface in the Telnet session.
- By default, commands of level 0 are available to Telnet users authenticated by password. For the command hierarchy and command views, refer to *CLI Operation* in this manual.

Telnetting to the Switching Engine from the Access Control Engine

You can Telnet to the switching engine from the access control engine. In this case, the access control engine operates as the client, and the switching engine operates as the server. If the interconnected Ethernet ports of the two engines are in the same LAN segment, make sure the IP addresses of the two management VLAN interfaces to which the two Ethernet ports belong are of the same network segment, or the route between the two VLAN interfaces is available.

As shown in Figure 3-8, after Telnetting to the access control engine (labeled as Telnet client), you can Telnet to the switching engine (labeled as Telnet server) by executing the **telnet** command and then configure it.

Figure 3-8 Network diagram for Telnetting to the switching engine from the access control engine



1) Perform Telnet-related configuration on the switching engine operating as the Telnet server. For details, refer to Telnet Configuration with Authentication Mode Being None, Telnet Configuration with Authentication Mode Being Password, and Telnet Configuration with Authentication Mode Being Scheme.
2) Telnet to the access control engine as the Telnet client.
3) Execute the following command on the access control engine operating as the Telnet client:

```
<device> telnet xxxx
```

Note that xxxx is the IP address or the host name of the access control engine operating as the Telnet server. You can use the **ip host** to assign a host name to the access control engine.

4) After successful login, the CLI prompt (such as <device>) appears. If all the VTY user interfaces of the switching engine are in use, you will fail to establish the connection and receive the message that says “All user interfaces are used, please try later!”.
5) After successfully Telnetting to the switching engine, you can configure the switching engine or display the information about the switching engine by executing corresponding commands. You can also type ? at any time for help. Refer to the subsequent chapters for the information about the commands.

4 Logging In from the Web-Based Network Management System

When logging in from the Web-based network management system, go to these sections for information you are interested in:

- Introduction
- Setting Up a Web Configuration Environment
- Configuring the Login Banner
- Enabling/Disabling the WEB Server

Introduction

The device has a Web server built in. It enables you to log in to switching engine from a Web browser and then manage and maintain the device intuitively by interacting with the built-in Web server.

To log in to the built-in Web-based network management system of the switching engine, you need to perform the related configuration on both the switching engine and the PC operating as the network management terminal.

Table 4-1 Requirements for logging in to the switching engine from the Web-based network management system

Item	Requirement
Switching engine	The VLAN interface of the switching engine is assigned an IP address, and the route between the switching engine and the Web network management terminal is reachable. (Refer to *IP Address and Performance Operation* and *Routing Protocol* parts for related information.)
	The user name and password for logging in to the Web-based network management system are configured.
PC operating as the network management terminal	IE is available.
	The IP address of the VLAN interface of the switching engine, the user name, and the password are available.

Setting Up a Web Configuration Environment

Note

Your WX series access controller products were delivered with a factory default configuration. This configuration allows you to log into the built-in Web-based management system of the access controller product from a Web browser on a PC by inputting **http://192.168.0.101** in the address bar of the browser. The default login username and password are both **admin**. After selecting your desired language, you can log in to the Web interface to make configuration. If you save your configuration, the device will boot with the configuration you made rather than the default at the next boot.

Log in to the switching engine with the **oap connect slot 0** command and then perform the following operations.

1) Assign an IP address to VLAN-interface 1 of the switching engine (VLAN 1 is the default VLAN of the switching engine), and create a user account for the login user.

Assign an IP address to the switching engine.

```
<device> system-view
[device] interface Vlan-interface 1
[device-Vlan-interface1] ip address 192.168.0.101 24
[device-Vlan-interface1] quit
```

Create a Web user account, setting both the user name and the password to **admin** and the user level to 3 (manage level).

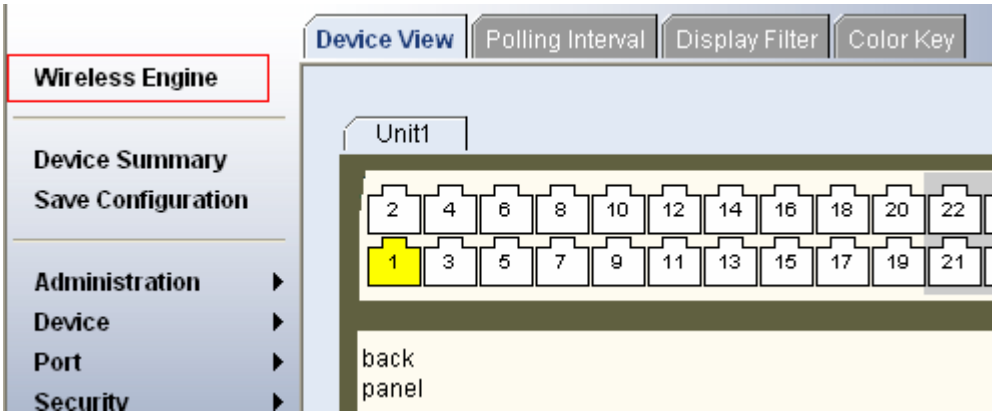
```
[device] local-user admin
[device-luser-admin] service-type telnet level 3
[device-luser-admin] password simple admin
[device-luser-admin] quit
```

2) Configure the management IP address for the switching engine of the device (Optional).

After configuring the IP address, you can go to the Web interface of the switching engine from the Web interface of the access controller engine by clicking the **Wireless Engine** button on the left upper part of the page, as shown in Figure 4-1. 192.168.0.100 is the management IP address of the switching engine, and slot 0 is the slot number of the switching engine.

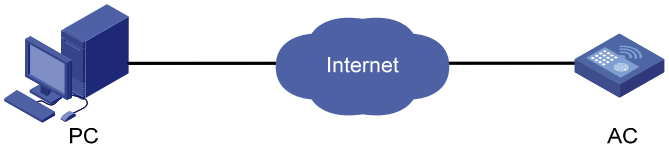
```
[device] oap management-ip 192.168.0.100 slot 0
```

Figure 4-1 Web interface of the access controller engine



3) Set up a Web configuration environment, as shown in Figure 4-2.

Figure 4-2 Set up a Web configuration environment



4) Log in to the switching engine through IE. Launch IE on the Web-based network management terminal (your PC) and enter http://192.168.0.101 in the address bar. (Make sure a route is available between the Web-based network management terminal and the switching engine.)
5) When the login authentication interface (as shown in Figure 4-3) appears, enter the user name and the password configured in step 2 and click **Login** to bring up the main page of the Web-based network management system.

Figure 4-3 The login page of the Web-based network management system



Configuring the Login Banner

Configuration Procedure

If a login banner is configured with the **header** command, when a user logs in through Web, the banner page is displayed before the user login authentication page. The contents of the banner page are the login banner information configured with the **header** command. Then, by clicking <Continue**>** on the banner page, the user can enter the user login authentication page, and enter the main page of the Web-based network management system after passing the authentication. If no login banner is

configured by the **header** command, a user logging in through Web directly enters the user login authentication page.

Follow these steps to configure the login banner:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the banner to be displayed when a user logs in through Web	**header login** *text*	Required By default, no login banner is configured.

Configuration Example

Network requirements

As shown in Figure 4-4,

- A user logs in to the switching engine through Web.
- The banner page is desired when a user logs in to the switching engine.

Figure 4-4 Network diagram for login banner configuration



Configuration Procedure

Enter system view.

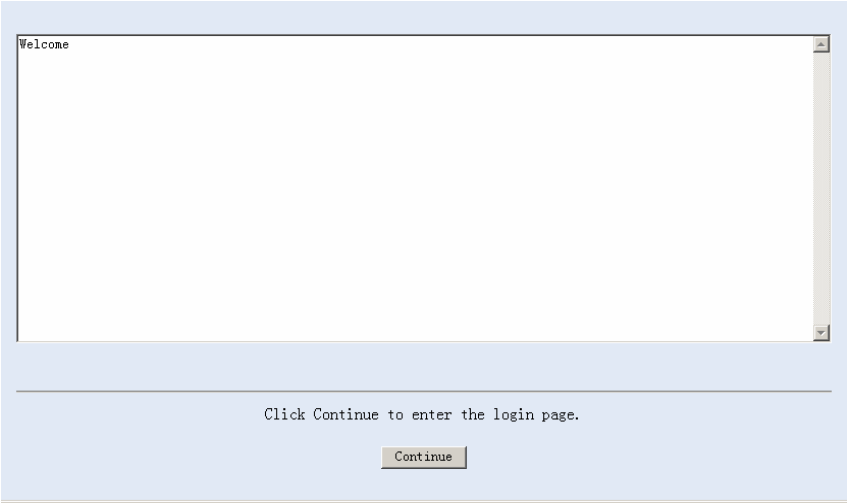
```
<device> system-view
```

Configure the banner "Welcome" to be displayed when a user logs in to the switching engine through Web.

```
[device] header login %Welcome%
```

Assume that a route is available between the user terminal (the PC) and the switching engine. After the above-mentioned configuration, if you enter the IP address of the switching engine in the address bar of the browser running on the user terminal and press <Enter>, the browser will display the banner page, as shown in Figure 4-5.

Figure 4-5 Banner page displayed when a user logs in to the switching engine through Web



Click **Continue** to enter user login authentication page. You will enter the main page of the Web-based network management system if the authentication succeeds.

Enabling/Disabling the WEB Server

Follow these steps to enable/disable the WEB server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the Web server	**ip http shutdown**	Required By default, the Web server is enabled.
Disable the Web server	**undo ip http shutdown**	Required

Note

To improve security and prevent attack to the unused Sockets, TCP 80 port (which is for HTTP service) is enabled/disabled after the corresponding configuration.

- Enabling the Web server (by using the **undo ip http shutdown** command) opens TCP 80 port.
- Disabling the Web server (by using the **ip http shutdown** command) closes TCP 80 port.

5 Logging In from NMS

Introduction

You can also log in to the switching engine from a network management station (NMS), and then configure and manage the switching engine through the agent module on the switch. Simple network management protocol (SNMP) is applied between the NMS and the agent. Refer to the *SNMP-RMON* part for related information.

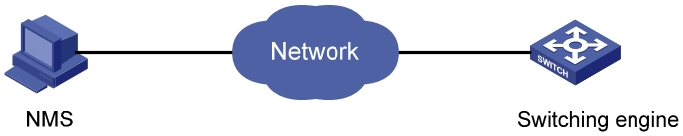
To log in to the switching engine from an NMS, you need to perform related configuration on both the NMS and the switching engine.

Table 5-1 Requirements for logging in to the switching engine from an NMS

Item	Requirement
Switching engine	The IP address of the VLAN interface of the switching engine is configured. The route between the NMS and the switching engine is reachable. (Refer to *IP Address and Performance Operation* and *Routing Protocol* parts for related information.)
	The basic SNMP functions are configured. (Refer to the *SNMP-RMON* part for related information.)
NMS	The NMS is properly configured. (Refer to the user manual of your NMS for related information.)

Connection Establishment Using NMS

Figure 5-1 Network diagram for logging in from an NMS



6 Configuring Source IP Address for Telnet Service Packets

Overview

You can configure source IP address or source interface for the Telnet server and Telnet client. This provides a way to manage services and enhances security.

The source IP address specified for Telnet service packets is the IP address of a Loopback interface or VLAN interface. After you specify the IP address of a virtual Loopback interface or an unused VLAN interface as the source IP address of Telnet service packets, the IP address is used as the source IP address no matter which interface of the switching engine is used to transmit packets between the Telnet client and the Telnet server. This conceals the IP address of the actual interface used. As a result, external attacks are guarded and the security is improved. On the other hand, you can configure the Telnet server to accept only Telnet service packets with specific source IP addresses to make sure specific users can log in to the switching engine.

Configuring Source IP Address for Telnet Service Packets

This feature can be configured in either user view or system view. The configuration performed in user view takes effect for only the current session, while the configuration performed in system view takes effect for all the following sessions.

Configuration in user view

Follow these steps to configure a source IP address for service packets in user view:

To do…	Use the command…	Remarks
Specify a source IP address for the Telnet client	**telnet** *remote-server* **source-ip** *ip-address*	Optional
Specify a source interface for the Telnet client	**telnet** *remote-server* **source-interface** *interface-type interface-number*	Optional

Configuration in system view

Follow these steps to configure a source IP address for service packets in system view:

To do…	Use the command…	Remarks
Specify a source IP address for Telnet server	**telnet-server source-ip** *ip-address*	Optional
Specify a source interface for Telnet server	**telnet-server source-interface** *interface-type interface-number*	Optional
Specify source IP address for Telnet client	**telnet source-ip** *ip-address*	Optional

To do…	Use the command…	Remarks
Specify a source interface for Telnet client	**telnet source-interface** *interface-type interface-number*	Optional

Note

When configuring a source IP address for Telnet packets, ensure that:

- The source IP address must be one on the local device.
- The source interface must already exist.
- A reachable route is available between the source IP address (or the source interface) specified for the Telnet server or client and the Telnet client or server.

Displaying Source IP Address Configuration

To do…	Use the command…	Remarks
Display the source IP address configured for the Telnet client	**display telnet source-ip**	Available in any view
Display the source IP address configured for the Telnet server	**display telnet-server source-ip**	

7 User Control

Note

Refer to the *ACL* part for information about ACL.

Introduction

The switching engine provides ways to control different types of login users, as listed in Table 7-1.

Table 7-1 Ways to control different types of login users

Login mode	Control method	Implementation	Reference
Telnet	By source IP address	Through basic ACLs	Controlling Telnet Users by Source IP Addresses.
	By source and destination IP address	Through advanced ACLs	Controlling Telnet Users by Source and Destination IP Addresses
	By source MAC address	Through Layer 2 ACLs	Controlling Telnet Users by Source MAC Addresses
SNMP	By source IP addresses	Through basic ACLs	Controlling Network Management Users by Source IP Addresses
WEB	By source IP addresses	Through basic ACLs	Controlling Web Users by Source IP Address
	Disconnect Web users by force	By executing commands at CLI	Disconnecting a Web User by Force

Controlling Telnet Users

Prerequisites

The controlling policy against Telnet users is determined, including the source IP addresses, destination IP addresses and source MAC addresses to be controlled and the controlling actions (permitting or denying).

Controlling Telnet Users by Source IP Addresses

Controlling Telnet users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Follow these steps to control Telnet users by source IP addresses:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a basic ACL or enter basic ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **deny | permit** } [*rule-string*]	Required
Quit to system view	**quit**	—
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	—
Apply the ACL to control Telnet users by source IP addresses	**acl** *acl-number* { **inbound** | **outbound** }	Required The **inbound** keyword specifies to filter the users trying to Telnet to the current switching engine. The **outbound** keyword specifies to filter users trying to Telnet to other devices from the current switching engine.

Controlling Telnet Users by Source and Destination IP Addresses

Controlling Telnet users by source and destination IP addresses is achieved by applying advanced ACLs, which are numbered from 3000 to 3999.

Follow these steps to control Telnet users by source and destination IP addresses:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create an advanced ACL or enter advanced ACL view	**acl number** *acl-number* [**match-order** { **config | auto** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [*rule-string*]	Required You can define rules as needed to filter by specific source and destination IP addresses.
Quit to system view	**quit**	—
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	—
Apply the ACL to control Telnet users by specified source and destination IP addresses	**acl** *acl-number* { **inbound** | **outbound** }	Required The **inbound** keyword specifies to filter the users trying to Telnet to the current switching engine. The **outbound** keyword specifies to filter users trying to Telnet to other devices from the current switching engine.

Controlling Telnet Users by Source MAC Addresses

Controlling Telnet users by source MAC addresses is achieved by applying Layer 2 ACLs, which are numbered from 4000 to 4999.

Follow these steps to control Telnet users by source MAC addresses:

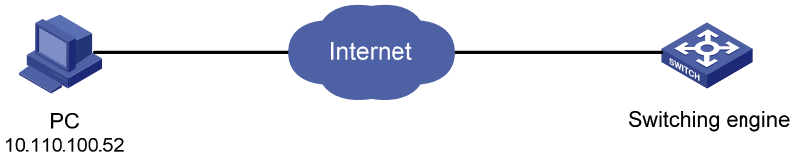
To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create or enter Layer 2 ACL view	**acl number** *acl-number*	—
Define rules for the ACL	**rule** [*rule-id*] { **deny** | **permit** } [*rule-string*]	Required You can define rules as needed to filter by specific source MAC addresses.
Quit to system view	**quit**	—
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	—
Apply the ACL to control Telnet users by specified source MAC addresses	**acl** *acl-number* **inbound**	Required By default, no ACL is applied for Telnet users.

Configuration Example

Network requirements

As shown in Figure 7-1, only the Telnet users sourced from the IP address of 10.110.100.52 are permitted to access the switching engine.

Figure 7-1 Network diagram for controlling Telnet users using ACLs



Configuration procedure

Define a basic ACL.

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[device-acl-basic-2000] quit
```

Apply the ACL.

```
[device] user-interface vty 0 4
[device-ui-vty0-4] acl 2000 inbound
```

Controlling Network Management Users by Source IP Addresses

You can manage the device through network management software. Network management users can access switching engines through SNMP.

You need to perform the following two operations to control network management users by source IP addresses.

- Defining an ACL
- Applying the ACL to control users accessing the switching engine through SNMP

Prerequisites

The controlling policy against network management users is determined, including the source IP addresses to be controlled and the controlling actions (permitting or denying).

Controlling Network Management Users by Source IP Addresses

Controlling network management users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Follow these steps to control network management users by source IP addresses:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a basic ACL or enter basic ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	Required As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **deny | permit** } [*rule-string*]	Required
Quit to system view	**quit**	—
Apply the ACL while configuring the SNMP community name	**snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name* | **acl** *acl-number*]*	Optional By default, SNMPv1 and SNMPv2c use community name to access.
Apply the ACL while configuring the SNMP group name	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*] **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	Optional By default, the authentication mode and the encryption mode are configured as none for the group.
Apply the ACL while configuring the SNMP user name	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*] **snmp-agent usm-user v3** *user-name group-name* [**cipher**] [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode des56** *priv-password*] [**acl** *acl-number*]	Optional

Note

You can specify different ACLs while configuring the SNMP community name, SNMP group name, and SNMP user name.

As SNMP community name is a feature of SNMPv1 and SNMPv2c, the specified ACLs in the command that configures SNMP community names (the **snmp-agent community** command) take effect in the network management systems that adopt SNMPv1 or SNMPv2c.

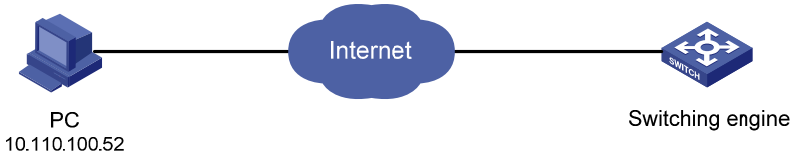
Similarly, as SNMP group name and SNMP username name are a feature of SNMPv2c and the higher SNMP versions, the specified ACLs in the commands that configure SNMP group names and SNMP user names take effect in the network management systems that adopt SNMPv2c or higher SNMP versions. If you specify ACLs in the commands, the network management users are filtered by the SNMP group name and SNMP user name.

Configuration Example

Network requirements

As shown in Figure 7-2, only SNMP users sourced from the IP addresses of 10.110.100.52 are permitted to log in to the switching engine.

Figure 7-2 Network diagram for controlling SNMP users using ACLs



Configuration procedure

Define a basic ACL.

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[device-acl-basic-2000] quit
```

Apply the ACL to only permit SNMP users sourced from the IP addresses of 10.110.100.52 to access the switching engine.

```
[device] snmp-agent community read aaa acl 2000
[device] snmp-agent group v2c groupa acl 2000
[device] snmp-agent usm-user v2c usera groupa acl 2000
```

Controlling Web Users by Source IP Address

You can manage the device remotely through Web. Web users can access the switching engine through HTTP connections.

You need to perform the following two operations to control Web users by source IP addresses.

- Defining an ACL

- Applying the ACL to control Web users

Prerequisites

The controlling policy against Web users is determined, including the source IP addresses to be controlled and the controlling actions (permitting or denying).

Controlling Web Users by Source IP Addresses

Controlling Web users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Follow these steps to control Web users by source IP addresses:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a basic ACL or enter basic ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **deny | permit** } [*rule-string*]	Required
Quit to system view	**quit**	—
Apply the ACL to control Web users	**ip http acl** *acl-number*	Optional By default, no ACL is applied for Web users.

Disconnecting a Web User by Force

The administrator can disconnect a Web user by force using the related commands.

Follow these steps to disconnect a Web user by force:

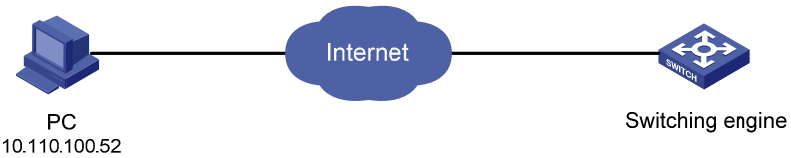
To do…	Use the command…	Remarks
Disconnect a Web user by force	**free web-users** { **all** | **user-id** *user-id* | **user-name** *user-name* }	Required Execute this command in user view.

Configuration Example

Network requirements

As shown in Figure 7-3, only the Web users sourced from the IP address of 10.110.100.52 are permitted to access the switching engine.

Figure 7-3 Network diagram for controlling Web users using ACLs



Configuration procedure

Define a basic ACL.

```
<device> system-view
[device] acl number 2030
[device-acl-basic-2030] rule 1 permit source 10.110.100.52 0
[device-acl-basic-2030] quit
```

Apply ACL 2030 to only permit the Web users sourced from the IP address of 10.110.100.52 to access the switching engine.

```
[device] ip http acl 2030
```

Table of Contents

1 Configuration File Management 1-1
Introduction to Configuration File 1-1
Management of Configuration File 1-2
Saving the Current Configuration 1-2
Erasing the Startup Configuration File 1-3
Specifying a Configuration File for Next Startup 1-4
Displaying and Maintaining Device Configuration 1-5

1 Configuration File Management

Note

The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Introduction to Configuration File

A configuration file records and stores user configurations performed to the device. It also enables users to check device configurations easily.

Types of configuration

The configuration of a device falls into two types:

- Saved configuration, a configuration file used for initialization. If this file does not exist, the device starts up without loading any configuration file.
- Current configuration, which refers to the user's configuration during the operation of a device. This configuration is stored in dynamic random-access memory (DRAM). It is removed when rebooting.

Format of configuration file

Configuration files are saved as text files for ease of reading. They:

- Save configuration in the form of commands.
- Save only non-default configuration settings.
- The commands are grouped into sections by command view. The commands that are of the same command view are grouped into one section. Sections are separated by comment lines. (A line is a comment line if it starts with the character "#".)
- The sections are listed in this order: system configuration section, logical interface configuration section, physical port configuration section, routing protocol configuration section, user interface configuration, and so on.
- End with a return.

The operating interface provided by the configuration file management function is user-friendly. With it, you can easily manage your configuration files.

Main/backup attribute of the configuration file

Main and backup indicate the main and backup attribute of the configuration file respectively. A main configuration file and a backup configuration file can coexist on the device. As such, when the main configuration file is missing or damaged, the backup file can be used instead. This increases the safety and reliability of the file system compared with the device that only support one configuration file. You

can configure a file to have both main and backup attribute, but only one file of either main or backup attribute is allowed on a device.

The following three situations are concerned with the main/backup attributes:

- When saving the current configuration, you can specify the file to be a main or backup or normal configuration file.
- When removing a configuration file from a device, you can specify to remove the main or backup configuration file. Or, if it is a file having both main and backup attribute, you can specify to erase the main or backup attribute of the file.
- When setting the configuration file for next startup, you can specify to use the main or backup configuration file.

Startup with the configuration file

When booting, the system chooses the configuration files following the rules below:

1) If the main configuration file exists, the device initializes with this configuration.
2) If the main configuration file does not exist but the backup configuration file exists, the device initializes with the backup configuration.
3) If neither the main nor the backup configuration file exists, the device starts up without loading the configuration file.

Management of Configuration File

Complete the following tasks to configure configuration file management:

Task	Remarks
Saving the Current Configuration	Optional
Erasing the Startup Configuration File	Optional
Specifying a Configuration File for Next Startup	Optional

Saving the Current Configuration

You can modify the configuration on your device at the command line interface (CLI). To use the modified configuration for your subsequent startups, you must save it (using the **save** command) as a configuration file.

Follow these steps to save current configuration:

To do…	Use the command…	Remarks
Save current configuration	**save** [*cfgfile* | [**safely**] [**backup** | **main**]]	Required Available in any view

Modes in saving the configuration

- Fast saving mode. This is the mode when you use the **save** command without the **safely** keyword. The mode saves the file quicker but is likely to lose the original configuration file if the device reboots or the power fails during the process.

- Safe mode. This is the mode when you use the **save** command with the **safely** keyword. The mode saves the file slower but can retain the original configuration file in the device even if the device reboots or the power fails during the process.

 **Caution**

The configuration file to be used for next startup may be lost if the device reboots or the power fails during the configuration file saving process. In this case, the device reboots without loading any configuration file. After the device reboots, you need to specify a configuration file for the next startup. Refer to Specifying a Configuration File for Next Startup for details.

Three attributes of the configuration file

- Main attribute. When you use the **save** [[**safely**] [**main**]] command to save the current configuration, the configuration file you get has main attribute. If this configuration file already exists and has backup attribute, the file will have both main and backup attributes after execution of this command. If the filename you entered is different from that existing in the system, this command will erase its main attribute to allow only one main attribute configuration file in the device.
- Backup attribute. When you use the **save** [**safely**] **backup** command to save the current configuration, the configuration file you get has backup attribute. If this configuration file already exists and has main attribute, the file will have both main and backup attributes after execution of this command. If the filename you entered is different from that existing in the system, this command will erase its backup attribute to allow only one backup attribute configuration file in the device.
- Normal attribute. When you use the **save** *cfgfile* command to save the current configuration, the configuration file you get has normal attribute if it is not an existing file. Otherwise, the attribute is dependent on the original attribute of the file.

 **Note**

- It is recommended to adopt the fast saving mode in the conditions of stable power and adopt the safe mode in the conditions of unstable power or remote maintenance.
- The extension name of the configuration file must be .cfg.

Erasing the Startup Configuration File

You can clear the configuration files saved on the device through commands. After you clear the configuration files, the device starts up without loading the configuration file the next time it is started up.

Follow these steps to erase the configuration file:

To do…	Use the command…	Remarks
Erase the startup configuration file from the storage device	**reset saved-configuration** [**backup** | **main**]	Required Available in user view

You may need to erase the configuration file for one of these reasons:

- After you upgrade software, the old configuration file does not match the new software.
- The startup configuration file is corrupted or not the one you needed.

The following two situations exist:

- While the **reset saved-configuration** [**main**] command erases the configuration file with main attribute, it only erases the main attribute of a configuration file having both main and backup attribute.
- While the **reset saved-configuration backup** command erases the configuration file with backup attribute, it only erases the backup attribute of a configuration file having both main and backup attribute.

Caution

This command will permanently delete the configuration file from the device.

Specifying a Configuration File for Next Startup

Follow the step below to specify a configuration file for next startup:

To do…	Use the command…	Remarks
Specify a configuration file for next startup	**startup saved-configuration** *cfgfile* [**backup** | **main**]	Required Available in user view

You can specify a configuration file to be used for the next startup and configure the main/backup attribute for the configuration file.

Assign main attribute to the startup configuration file

- If you save the current configuration to the main configuration file, the system will automatically set the file as the main startup configuration file.
- You can also use the **startup saved-configuration** *cfgfile* [**main**] command to set the file as main startup configuration file.

Assign backup attribute to the startup configuration file

- If you save the current configuration to the backup configuration file, the system will automatically set the file as the backup startup configuration file.
- You can also use the **startup saved-configuration** *cfgfile* **backup** command to set the file as backup startup configuration file.

Note

The configuration file must use ".cfg" as its extension name and the startup configuration file must be saved at the root directory of the device.

Displaying and Maintaining Device Configuration

To do…	Use the command…	Remarks
Display the initial configuration file saved in the storage device	**display saved-configuration** [**unit** *unit-id*] [**by-linenum**]	Available in any view
Display the configuration file used for this and next startup	**display startup** [**unit** *unit-id*]	
Display the current VLAN configuration of the device	**display current-configuration vlan** [*vlan-id*] [**by-linenum**]	
Display the validated configuration in current view	**display this** [**by-linenum**]	
Display current configuration	**display current-configuration** [**configuration** [*configuration-type*] | **interface** [*interface-type*] [*interface-number*]] [**by-linenum**] [**|** { **begin** | **include** | **exclude** } *regular-expression*]	

Table of Contents

1 VLAN Overview 1-1
VLAN Overview 1-1
Introduction to VLAN 1-1
Advantages of VLANs 1-2
How VLAN Works 1-2
VLAN Interface 1-4
VLAN Classification 1-4
Port-Based VLAN 1-4
Protocol-Based VLAN 1-5
Introduction to Protocol-Based VLAN 1-5
Encapsulation Format of Ethernet Data 1-5
Procedure for the Switch to Judge Packet Protocol 1-7
Encapsulation Formats 1-7
Implementation of Protocol-Based VLAN 1-7

2 VLAN Configuration 2-1
VLAN Configuration 2-1
Configuration Task List 2-1
Basic VLAN Configuration 2-1
Basic VLAN Interface Configuration 2-2
Displaying and Maintaining VLAN 2-2
Configuring a Port-Based VLAN 2-3
Configuring a Port-Based VLAN 2-3
Protocol-Based VLAN Configuration Example 2-3
Configuring a Protocol-Based VLAN 2-5
Configuration Task List 2-5
Configuring a Protocol Template for a Protocol-Based VLAN 2-5
Associating a Port with a Protocol-Based VLAN 2-6
Displaying and Maintaining Protocol-Based VLAN 2-7
Protocol-Based VLAN Configuration Example 2-7

1 VLAN Overview



Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

VLAN Overview

Introduction to VLAN

The traditional Ethernet is a broadcast network, where all hosts are in the same broadcast domain and connected with each other through hubs or switches. Hubs and switches, which are the basic network connection devices, have limited forwarding functions.

- A hub is a physical layer device without the switching function, so it forwards the received packet to all ports except the inbound port of the packet.
- A switch is a link layer device which can forward a packet according to the MAC address of the packet. However, when the switch receives a broadcast packet or an unknown unicast packet whose MAC address is not included in the MAC address table of the switch, it will forward the packet to all the ports except the inbound port of the packet.

The above scenarios could result in the following network problems.

- Large quantity of broadcast packets or unknown unicast packets may exist in a network, wasting network resources.
- A host in the network receives a lot of packets whose destination is not the host itself, causing potential serious security problems.

Isolating broadcast domains is the solution for the above problems. The traditional way is to use routers, which forward packets according to the destination IP address and does not forward broadcast packets in the link layer. However, routers are expensive and provide few ports, so they cannot split the network efficiently. Therefore, using routers to isolate broadcast domains has many limitations.

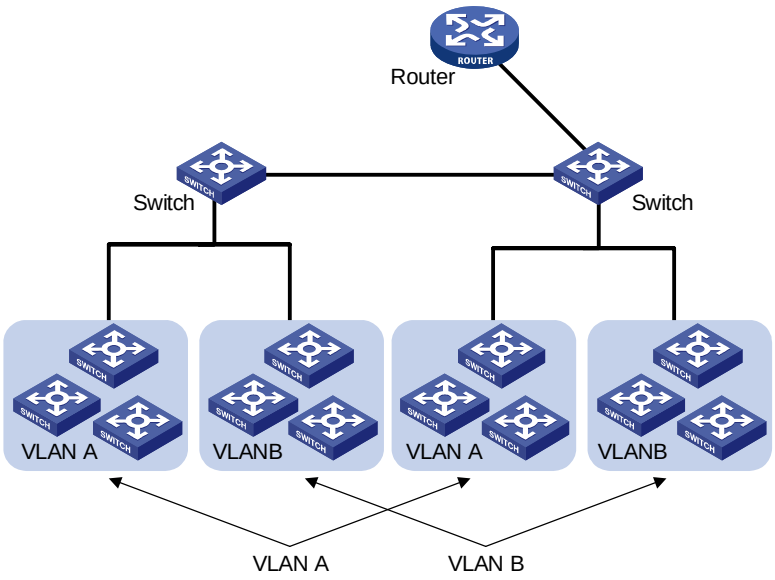
The virtual local area network (VLAN) technology is developed for switches to control broadcasts in LANs.

A VLAN can span across physical spaces. This enables hosts in a VLAN to be located in different physical locations.

By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own. Hosts in the same VLAN communicate in the traditional Ethernet way. However, hosts in different VLANs cannot communicate with each other directly but need the help

of network layer devices, such as routers and Layer 3 switches. Figure 1-1 illustrates a VLAN implementation.

Figure 1-1 A VLAN implementation



Advantages of VLANs

Compared with the traditional Ethernet, VLAN enjoys the following advantages.

- Broadcasts are confined to VLANs. This decreases bandwidth consumption and improves network performance.
- Network security is improved. Because each VLAN forms a broadcast domain, hosts in different VLANs cannot communicate with each other directly unless routers or Layer 3 switches are used.
- A more flexible way to establish virtual workgroups. VLAN can be used to create a virtual workgroup spanning physical network segments. When the physical position of a host changes within the range of the virtual workgroup, the host can access the network without changing its network configuration.

How VLAN Works

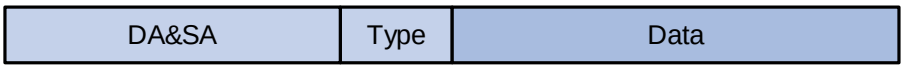
VLAN tag

VLAN tags in the packets are necessary for a switch to identify packets of different VLANs. A switch works at the data link layer of the OSI model (Layer 3 switches are not discussed in this chapter) and it can identify the data link layer encapsulation of the packet only, so you need to add the VLAN tag field into the data link layer encapsulation if necessary.

In 1999, IEEE issues the IEEE 802.1Q protocol to standardize VLAN implementation, defining the structure of VLAN-tagged packets.

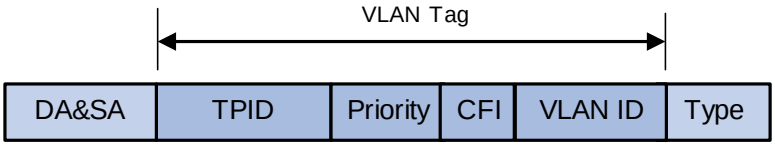
In traditional Ethernet data frames, the type field of the upper layer protocol is encapsulated after the destination MAC address and source MAC address, as shown in Figure 1-2

Figure 1-2 Encapsulation format of traditional Ethernet frames



In Figure 1-2 DA refers to the destination MAC address, SA refers to the source MAC address, and Type refers to the upper layer protocol type of the packet. IEEE 802.1Q protocol defines that a 4-byte VLAN tag is encapsulated after the destination MAC address and source MAC address to show the information about VLAN.

Figure 1-3 Format of VLAN tag



As shown in Figure 1-3, a VLAN tag contains four fields, including the tag protocol identifier (TPID), priority, canonical format indicator (CFI), and VLAN ID.

- TPID is a 16-bit field, indicating that this data frame is VLAN-tagged. By default, it is 0x8100 in the WX3000 series devices.
- Priority is a 3-bit field, referring to 802.1p priority. Refer to the “QoS-QoS profile” part of this manual for details.
- CFI is a 1-bit field, indicating whether the MAC address is encapsulated in the standard format. 0 (the value of the CFI filed) indicates the MAC address is encapsulated in the standard format and 1 indicates the MAC address is not encapsulated in the standard format. The value is 0 by default.
- VLAN ID is a 12-bit field, indicating the ID of the VLAN to which this packet belongs. It is in the range of 0 to 4,095. Generally, 0 and 4,095 is not used, so the field is in the range of 1 to 4,094.

Note

The frame format here takes the Ethernet II encapsulation as an example. Ethernet also supports 802.2/802.3 encapsulation, where VLAN tag is also encapsulated after the DA and SA field. Refer to Encapsulation Format of Ethernet Data for 802.2/802.3 encapsulation format.

VLAN ID identifies the VLAN to which a packet belongs. When a switch receives a packet carrying no VLAN tag, the switch encapsulates a VLAN tag with the default VLAN ID of the inbound port for the packet, and sends the packet to the default VLAN of the inbound port for transmission. For the details about setting the default VLAN of a port, refer to the default VLAN ID configuration of a port section in the “Port Basic Configuration” part of the manual.

MAC address learning mechanism of VLANs

Switches forward packets according to the destination MAC addresses of the packets. So that switches maintain a table called MAC address forwarding table to record the source MAC addresses of the received packets and the corresponding ports receiving the packets for consequent packet forwarding. The process of recording is called MAC address learning.

After VLANs are configured on a switch, the MAC address learning of the switch has the following two modes.

- Shared VLAN learning (SVL): the switch records all the MAC address entries learnt by ports in all VLANs to a shared MAC address forwarding table. Packets received on any port of any VLAN are forwarded according to this table.
- Independent VLAN learning (IVL): the switch maintains an independent MAC address forwarding table for each VLAN. The source MAC address of a packet received on a port of a VLAN is recorded to the MAC address forwarding table of this VLAN only, and packets received on a port of a VLAN are forwarded according to the VLAN's own MAC address forwarding table.

Currently, the device adopts the IVL mode only. For more information about the MAC address forwarding table, refer to the "MAC Address Forwarding Table Management" part of the manual.

VLAN Interface

Hosts in different VLANs cannot communicate with each other directly unless routers or Layer 3 switches are used to do Layer 3 forwarding. The device supports VLAN interfaces configuration to forward packets in Layer 3.

VLAN interface is a virtual interface in Layer 3 mode, used to realize the layer 3 communication between different VLANs, and does not exist on a switch as a physical entity. Each VLAN has a VLAN interface, which can forward packets of the local VLAN to the destination IP addresses at the network layer. Normally, since VLANs can isolate broadcast domains, each VLAN corresponds to an IP network segment. And a VLAN interface serves as the gateway of the segment to forward packets in Layer 3 based on IP addresses.

 **Note**

The switching engine used in the device can be configured with a maximum number of eight VLAN interfaces.

VLAN Classification

Depending on how VLANs are established, VLANs fall into the following six categories.

- Port-based VLANs
- MAC address-based VLANs
- Protocol-based VLANs
- IP-subnet-based VLANs
- Policy-based VLANs
- Other types

Port-Based VLAN

Port-based VLAN technology introduces the simplest way to classify VLANs. You can assign the ports on the device to different VLANs. Thus packets received on a port will be transmitted through the corresponding VLAN only, so as to isolate hosts to different broadcast domains and divide them into different virtual workgroups.

The link type of a port on the device can be one of the following: access, trunk, and hybrid. For the three types of ports, the process of being added into a VLAN and the way of forwarding packets are different. For details, refer to the “Port Basic Configuration” part of the manual.

Port-based VLANs are easy to implement and manage and applicable to hosts with relatively fixed positions.

Protocol-Based VLAN

Introduction to Protocol-Based VLAN

Protocol-based VLAN is also known as protocol VLAN, which is another way to classify VLANs. Through the protocol-based VLANs, the switch can analyze the received packets carrying no VLAN tag on the port and match the packets with the user-defined protocol template automatically according to different encapsulation formats and the values of specific fields. If a packet is matched, the switch will add a corresponding VLAN tag to it automatically. Thus, data of specific protocol is assigned automatically to the corresponding VLAN for transmission.

This feature is used for binding the types of services provided in the network to VLANs to facilitate management and maintenance.

Encapsulation Format of Ethernet Data

This section introduces the common encapsulation formats of Ethernet data for you to understand well the procedure for the switch to identify the packet protocols.

Ethernet II and 802.2/802.3 encapsulation

Mainly, there are two encapsulation types of Ethernet packets: Ethernet II and 802.2/802.3, defined by RFC 894 and RFC 1042 respectively. The two encapsulation formats are described in the following figures.

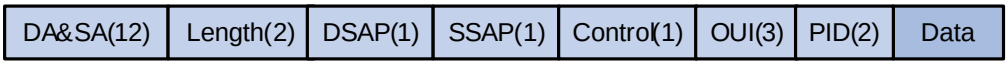
- Ethernet II packet:

Figure 1-4 Ethernet II encapsulation format



- 802.2/802.3 packet:

Figure 1-5 802.2/802.3 encapsulation format



In the two figures, DA and SA refer to the destination MAC address and source MAC address of the packet respectively. The number in the bracket indicates the field length in bytes.

The maximum length of an Ethernet packet is 1500 bytes, that is, 0x05DC in hexadecimal, so the length field in 802.2/802.3 encapsulation is in the range of 0x0000 to 0x05DC.

Whereas, the type field in Ethernet II encapsulation is in the range of 0x0600 to 0xFFFF.

Packets with the value of the type or length field being in the range 0x05DD to 0x05FF are regarded as illegal packets and thus discarded directly.

The switch identifies whether a packet is an Ethernet II packet or an 802.2/802.3 packet according to the ranges of the two fields.

Extended encapsulation formats of 802.2/802.3 packets

802.2/802.3 packets have the following three extended encapsulation formats:

- 802.3 raw encapsulation: only the length field is encapsulated after the source and destination address field, followed by the upper layer data. No other fields are included.

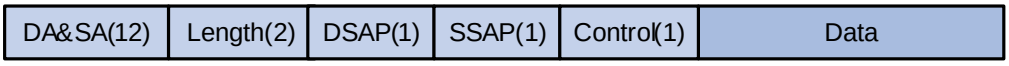
Figure 1-6 802.3 raw encapsulation format



Currently, only the IPX protocol supports 802.3 raw encapsulation, featuring with the value of the two bytes after the length field being 0xFFFF.

- 802.2 logical link control (LLC) encapsulation: the length field, the destination service access point (DSAP) field, the source service access point (SSAP) field and the control field are encapsulated after the source and destination address field. The value of the control field is always 3.

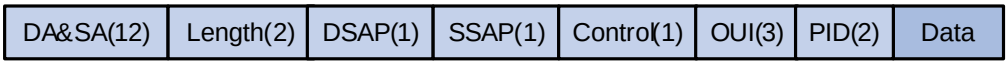
Figure 1-7 802.2 LLC encapsulation format



The DSAP field and the SSAP field in the 802.2 LLC encapsulation are used to identify the upper layer protocol. For example, if the two fields are both 0xE0, the upper layer protocol is IPX protocol.

- 802.2 sub-network access protocol (SNAP) encapsulation: encapsulates packets according to the 802.3 standard packet format, including the length, DSAP, SSAP, control, organizationally unique identifier (OUI), and protocol-ID (PID) fields.

Figure 1-8 802.2 SNAP encapsulation format



In 802.2 SNAP encapsulation format, the values of the DSAP field and the SSAP field are always 0xAA, and the value of the control field is always 3.

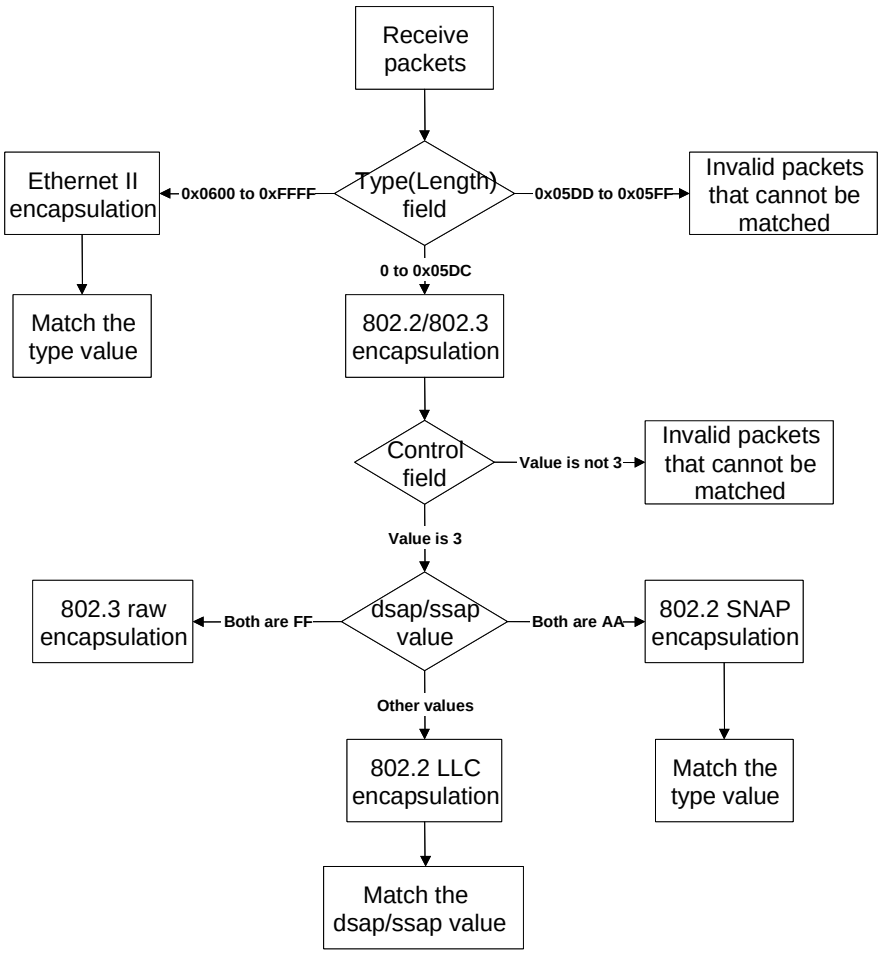
The switch differentiates between 802.2 LLC encapsulation and 802.2 SNAP encapsulation according to the values of the DSAP field and the SSAP field.

Note

When the OUI is 00-00-00 in 802.2 SNAP encapsulation, the PID field has the same meaning as the type field in Ethernet II encapsulation, which both refer to globally unique protocol number. Such encapsulation is also known as SNAP RFC1042 encapsulation, which is standard SNAP encapsulation. The SNAP encapsulation mentioned in this chapter refers to SNAP RFC 1042 encapsulation.

Procedure for the Switch to Judge Packet Protocol

Figure 1-9 Procedure for the switch to judge packet protocol



Encapsulation Formats

Table 1-1 lists the encapsulation formats supported by some protocols. In brackets are type values of these protocols.

Table 1-1 Encapsulation formats

Encapsulation / Protocol	Ethernet II	802.3 raw	802.2 LLC	802.2 SNAP
IP (0x0800)	Supported	Not supported	Not supported	Supported
IPX (0x8137)	Supported	Supported	Supported	Supported
AppleTalk (0x809B)	Supported	Not supported	Not supported	Supported

Implementation of Protocol-Based VLAN

The switching engines of the devices assign the packet to the specific VLAN by matching the packet with the protocol template.

The protocol template is the standard to determine the protocol to which a packet belongs. Protocol templates include standard templates and user-defined templates:

- The standard template adopts the RFC-defined packet encapsulation formats and values of some specific fields as the matching criteria.
- The user-defined template adopts the user-defined encapsulation formats and values of some specific fields as the matching criteria.

After configuring the protocol template, you must add a port to the protocol-based VLAN and associate this port with the protocol template. This port will add VLAN tags to the packets based on protocol types. The port in the protocol-based VLAN must be connected to a client. However, a common client cannot process VLAN-tagged packets. In order that the client can process the packets out of this port, you must configure the port in the protocol-based VLAN as a hybrid port and configure the port to remove VLAN tags when forwarding packets of all VLANs.



Note

For the operation of removing VLAN tags when the hybrid port sends packets, refer to the section “Port Basic Configuration” in this manual.

---

2 VLAN Configuration

VLAN Configuration

Configuration Task List

Complete the following tasks to configure VLAN:

Task	Remarks
Basic VLAN Configuration	Required
Basic VLAN Interface Configuration	Optional
Displaying and Maintaining VLAN	Optional

Basic VLAN Configuration

Follow these steps to make basic VLAN configuration:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create multiple VLANs in batch	**vlan** { *vlan-id1* **to** *vlan-id2* | **all** }	Optional
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	Required By default, there is only one VLAN, that is, the default VLAN (VLAN 1).
Assign a name for the current VLAN	**name** *text*	Optional By default, the name of a VLAN is its VLAN ID. “VLAN 0001” for example.
Specify the description string of the current VLAN	**description** *text*	Optional By default, the description string of a VLAN is its VLAN ID. “VLAN 0001” for example.

Caution

- VLAN 1 is the system default VLAN, which needs not to be created and cannot be removed, either.
- The VLAN you created in the way described above is a static VLAN. On the switch, there are dynamic VLANs which are registered through GVRP. For details, refer to “GVRP” part of this manual.
- When you use the **vlan** command to create VLANs, if the destination VLAN is an existing dynamic VLAN, it will be transformed into a static VLAN and the switch will output the prompt information.

Basic VLAN Interface Configuration

Configuration prerequisites

Before configuring a VLAN interface, create the corresponding VLAN.

Configuration procedure

Follow these steps to make basic VLAN interface configuration:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a VLAN interface and enter VLAN interface view	**interface Vlan-interface** *vlan-id*	Required By default, there is no VLAN interface on a switch.
Specify the description string for the current VLAN interface	**description** *text*	Optional By default, the description string of a VLAN interface is the name of this VLAN interface. “Vlan-interface1 Interface” for example.
Disable the VLAN interface	**shutdown**	Optional By default, the VLAN interface is enabled. In this case, the VLAN interface’s status is determined by the status of the ports in the VLAN, that is, if all ports of the VLAN are down, the VLAN interface is down (disabled); if one or more ports of the VLAN are up, the VLAN interface is up (enabled). If you disable the VLAN interface, the VLAN interface will always be down, regardless of the status of the ports in the VLAN.
Enable the VLAN Interface	**undo shutdown**	

Note

The operation of enabling/disabling a VLAN’s VLAN interface does not influence the physical status of the Ethernet ports belonging to this VLAN.

Displaying and Maintaining VLAN

To do…	Use the command…	Remarks
Display the VLAN interface information	**display interface Vlan-interface** [*vlan-id*]	Available in any view
Display the VLAN information	**display vlan** [*vlan-id* [**to** *vlan-id*] | **all** | **dynamic** | **static**]	

Configuring a Port-Based VLAN

Configuring a Port-Based VLAN

Configuration prerequisites

Create a VLAN before configuring a port-based VLAN.

Configuration procedure

Follow these steps to configure a port-based VLAN:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	—
Add Ethernet ports to the specific VLAN	**port** *interface-list*	Required By default, all the ports belong to the default VLAN (VLAN 1).

Caution

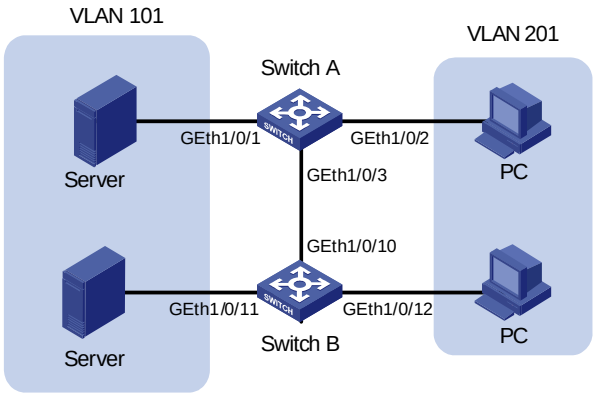
The commands above are effective for access ports only. If you want to add trunk ports or hybrid ports to a VLAN, you need to use the **port trunk permit vlan** command or the **port hybrid vlan** command in Ethernet port view. For the configuration procedure, refer to the section of configuring Ethernet ports in the "Port Basic Configuration" part of the manual.

Protocol-Based VLAN Configuration Example

Network requirements

- As shown in Figure 2-1, Switch A and Switch B each connect to a server and a workstation (PC).
- For data security concerns, the two servers are assigned to VLAN 101 with the descriptive string being “DMZ”, and the PCs are assigned to VLAN 201.
- The devices within each VLAN can communicate with each other but that in different VLANs cannot communicate with each other directly.

Figure 2-1 Network diagram for VLAN configuration



Configuration procedure

- Configure Switch A.

Create VLAN 101, specify its descriptive string as “DMZ”, and add GigabitEthernet 1/0/1 to VLAN 101.

```
<SwitchA> system-view
[SwitchA] vlan 101
[SwitchA-vlan101] description DMZ
[SwitchA-vlan101] port GigabitEthernet 1/0/1
[SwitchA-vlan101] quit
```

Create VLAN 201, and add GigabitEthernet 1/0/2 to VLAN 201.

```
[SwitchA] vlan 201
[SwitchA-vlan201] port GigabitEthernet 1/0/2
[SwitchA-vlan201] quit
```

- Configure Switch B.

Create VLAN 101, specify its descriptive string as “DMZ”, and add GigabitEthernet 1/0/11 to VLAN 101.

```
<SwitchB> system-view
[SwitchB] vlan 101
[SwitchB-vlan101] description DMZ
[SwitchB-vlan101] port GigabitEthernet 1/0/11
[SwitchB-vlan101] quit
```

Create VLAN 201, and add GigabitEthernet 1/0/12 to VLAN 201.

```
[SwitchB] vlan 201
[SwitchB-vlan201] port GigabitEthernet 1/0/12
[SwitchB-vlan201] quit
```

- Configure the link between Switch A and Switch B.

Because the link between Switch A and Switch B need to transmit data of both VLAN 101 and VLAN 102, you can configure the ports at the end of the link as trunk ports and permit packets of the two VLANs to pass through.

Configure GigabitEthernet 1/0/3 of Switch A.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 101
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 201
```

Configure GigabitEthernet 1/0/10 of Switch B.

```
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port link-type trunk
[SwitchB-GigabitEthernet1/0/10] port trunk permit vlan 101
[SwitchB-GigabitEthernet1/0/10] port trunk permit vlan 201
```

Note

For the command of configuring a port link type (**port link-type**) and the command of allowing packets of certain VLANs to pass through a port (**port trunk permit**), refer to the section of configuring Ethernet ports in the “Port Basic Configuration” part of this document.

Configuring a Protocol-Based VLAN

Configuration Task List

Complete the following tasks to configure protocol-based VLAN:

Task	Remarks
Configuring a Protocol Template for a Protocol-Based VLAN	Required
Associating a Port with a Protocol-Based VLAN	Required
Displaying and Maintaining Protocol-Based VLAN	Optional

Configuring a Protocol Template for a Protocol-Based VLAN

Configuration prerequisites

Create a VLAN before configuring the VLAN as a protocol-based VLAN.

Configuration procedure

Follow these steps to configure the protocol template for a VLAN:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	—
Configure the protocol template for the VLAN	**protocol-vlan** [*protocol-index*] { **at** | **ip** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc dsap** *dsap-id* **ssap** *ssap-id* | **snap etype** *etype-id* } }	Required By default, no protocol template is configured for the VLAN.

When configuring a protocol template for a protocol-based VLAN, use the **at**, **ip** or **ipx** keyword to configure a standard template to match AppleTalk, IP, and IPX packets respectively, and use the **mode** keyword to configure a user-defined template.

Caution

- Because the IP protocol is closely associated with the ARP protocol, you are recommended to configure the ARP protocol type when configuring the IP protocol type and associate the two protocol types with the same port to avoid that ARP packets and IP packets are not assigned to the same VLAN, which will cause IP address resolution failure.
- If you specify some special values for both the *dsap-id* and *ssap-id* arguments when configuring the user-defined template for **llc** encapsulation, the matching packets will take the same encapsulation format as some standard type of packets. For example, when both *dsap-id* and *ssap-id* have a value of 0xFF, the encapsulation format will be the same as that of **ipx raw** packets; if they both have a value of 0xE0, the packet encapsulation format will be the same as that of **ipx llc** packets; if they both have a value of 0xAA, the packet encapsulation format will be the same as that of **snap** packets. To prevent two commands from processing packets of the same protocol type in different ways, the system does not allow you to set both the *dsap-id* and *ssap-id* arguments to 0xFF, 0xE0, or 0xAA.
- When you use the **mode** keyword to configure a user-defined protocol template, if you set the *etype-id* argument for **ethernetii** or **snap** packets to 0x0800, 0x809B, or 0x8137, the matching packets will take the same format as that of the IP, IPX, and AppleTalk packets respectively. To prevent two commands from processing packets of the same protocol type in different ways, the switch will prompt that you cannot set the *etype-id* argument for **Ethernet II** or **snap** packets to 0x0800, 0x089B, or 0x8137.

Associating a Port with a Protocol-Based VLAN

Configuration prerequisites

- The protocol template for the protocol-based VLAN is configured.
- The port is configured as a hybrid port, and the port is configured to remove VLAN tags when it forwards the packets of the protocol-based VLANs.

Configuration procedure

Follow these steps to associate a port with the protocol-based VLAN:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter port view	**interface** *interface-type interface-number*	—
Associate the port with the specified protocol-based VLAN	**port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-index-end*] | **all** }	Required By default, a port is not associated with any protocol-based VLAN.

Note

For the operation of adding a hybrid port to a VLAN in the untagged way (when forwarding a packet, the port removes the VLAN tag of the packet), refer to the section of configuring Ethernet ports in the “Port Basic Configuration” part of this manual.

Displaying and Maintaining Protocol-Based VLAN

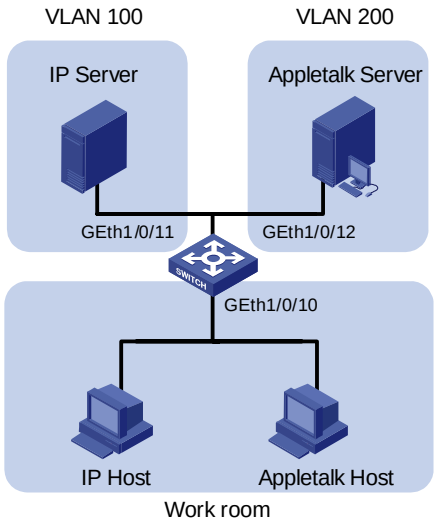
To do…	Use the command…	Remarks
Display the information about the protocol-based VLAN	**display vlan** [*vlan-id* [**to** *vlan-id*] | **all** | **dynamic** | **static**]	Available in any view
Display the protocol information and protocol indexes configured on the specified VLAN	**display protocol-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** }	
Display the protocol information and protocol indexes configured on the specified port	**display protocol-vlan interface** { *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

Protocol-Based VLAN Configuration Example

Network requirements

- As shown in Figure 2-2, Workroom connects to the LAN through port GigabitEthernet 1/0/10 on the switch.
- IP network and AppleTalk network workstations (hosts) coexist in the Workroom.
- The switch connects to VLAN 100 (using IP network) through GigabitEthernet 1/0/11 and to VLAN 200 (using AppleTalk network) through GigabitEthernet 1/0/12.
- Configure the switch to automatically assign the IP and AppleTalk packets to proper VLANs for transmission, so as to ensure the normal communication between the workstations and servers.

Figure 2-2 Network diagram for protocol-based VLAN configuration



Configuration procedure

Create VLAN 100 and VLAN 200, and add GigabitEthernet 1/0/11 and GigabitEthernet 1/0/12 to VLAN 100 and VLAN 200 respectively.

```
<device> system-view
[device] vlan 100
[device-vlan100] port GigabitEthernet 1/0/11
[device-vlan100] quit
[device] vlan 200
[device-vlan200] port GigabitEthernet 1/0/12
```

Configure protocol templates for VLAN 200 and VLAN 100, matching AppleTalk protocol and IP protocol respectively.

```
[device-vlan200] protocol-vlan at
[device-vlan200] quit
[device] vlan 100
[device-vlan100] protocol-vlan ip
```

To ensure the normal operation of IP network, you need to configure a user-defined protocol template for VLAN 100 to match the ARP protocol (assume Ethernet II encapsulation is adopted here).

```
[device-vlan100] protocol-vlan mode ethernetii etype 0806
```

Display the created protocol-based VLANs and the protocol templates.

```
[device-vlan100] display protocol-vlan vlan all
 VLAN ID: 100
 VLAN Type: Protocol-based VLAN
      Protocol Index        Protocol Type
             0                  ip
             1                  ethernetii etype 0x0806


 VLAN ID: 200
 VLAN Type: Protocol-based VLAN
      Protocol Index        Protocol Type
             0                  at
```

Configure GigabitEthernet 1/0/10 as a hybrid port, which removes the VLAN tag of the packets of VLAN 100 and VLAN 200 before forwarding the packets.

```
[device-vlan100] quit
[device] interface GigabitEthernet 1/0/10
[device-GigabitEthernet1/0/10] port link-type hybrid
[device-GigabitEthernet1/0/10] port hybrid vlan 100 200 untagged
```

Associate GigabitEthernet 1/0/10 with protocol template 0 and 1 of VLAN 100, and protocol template 0 of VLAN 200.

```
[device-GigabitEthernet1/0/10] port hybrid protocol-vlan vlan 100 0 to 1
[device-GigabitEthernet1/0/10] port hybrid protocol-vlan vlan 200 0
```

Display the associations between GigabitEthernet 1/0/10 and the VLAN protocol templates to verify your configuration.

```
[device-GigabitEthernet1/0/10] display protocol-vlan interface GigabitEthernet 1/0/10
 Interface:GigabitEthernet1/0/10
```

```
VLAN ID      Protocol-Index     Protocol-Type
    100             0               ip
    100             1               ethernetii etype 0x0806
    200             0               at
```

The above output information indicates that GigabitEthernet 1/0/10 has already been associated with the corresponding protocol templates of VLAN 100 and VLAN 200. Thus, packets from the IP and AppleTalk workstations can be automatically assigned to VLAN 100 and VLAN 200 respectively for transmission by matching the corresponding protocol templates, so as to realize the normal communication between the workstations and the servers.

Table of Contents

1 Auto Detect Configuration 1-1
Introduction to the Auto Detect Function 1-1
Auto Detect Configuration 1-2
Auto Detect Basic Configuration 1-2
Auto Detect Implementation in Static Routing 1-3
Auto Detect Implementation in VLAN Interface Backup 1-3
Auto Detect Configuration Examples 1-4
Configuration Example for Auto Detect Implementation in Static Routing 1-4
Configuration Example for Auto Detect Implementation in VLAN Interface Backup 1-5

1 Auto Detect Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

When configuring the auto detect function, go to these sections for information you are interested in:

- Introduction to the Auto Detect Function
- Auto Detect Configuration
- Auto Detect Configuration Examples

Introduction to the Auto Detect Function

The Auto Detect function uses ICMP request/reply packets to test network connectivity regularly.

The detected object of the Auto Detect function is a detected group, which is a set of IP addresses. To check the reachability to a detected group, a device enabled with Auto Detect sends ICMP requests to the group and waits for the ICMP replies from the group based on the user-defined policy (which includes the number of ICMP requests and the timeout waiting for a reply). Then according to the check result, the device determines whether to make the applications using the detected group take effect.

Currently, the following features are used in conjunction with Auto Detect:

- Static route
- Interface backup

Note

- A detected group can be used by multiple applications simultaneously.
- For details about static routing, refer to the Routing Protocol part of the manual.

Auto Detect Configuration

Complete the following tasks to configure auto detect:

Task	Remarks
Auto Detect Basic Configuration	Required
Auto Detect Implementation in Static Routing	Optional
Auto Detect Implementation in VLAN Interface Backup	Optional

Auto Detect Basic Configuration

Follow these steps to configure the auto detect function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a detected group and enter detected group view	**detect-group** *group-number*	Required
Add an IP address to be detected to the detected group	**detect-list** *list-number* **ip address** *ip-address* [**nexthop** *ip-address*]	Required
Specify a relationship between detected IP addresses in the group	**option** [**and** | **or**]	Optional By default, the **and** keyword is specified.
Set an interval between detecting operations	**timer loop** *interval*	Optional By default, the detecting interval is 15 seconds.
Set the number of ICMP requests during a detecting operation	**retry** *retry-times*	Optional By default, the number is 2.
Set a timeout waiting for an ICMP reply	**timer wait** *seconds*	Optional By default, the timeout is 2 seconds.
Display the detected group configuration	**display detect-group** [*group-number*]	Available in any view

Note

If the relationship between IP addresses of a detected group is **and**, any unreachable IP address in the group makes the detected group unreachable and the remaining IP addresses will not be detected. If the relationship is **or**, any reachable IP address makes the detected group reachable and the remaining IP addresses will not be detected.

Auto Detect Implementation in Static Routing

You can bind a static route with a detected group. The Auto Detect function will then detect the reachability of the static route through the path specified in the detected group.

- The static route is valid if the detected group is **reachable**.
- The static route is invalid if the detected group is **unreachable**.

Note

You need to create the detected group before performing the following operations.

Follow these steps to configure the auto detect function for a static route:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Bind a detected group to a static route	**ip route-static** *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-hop* } [**preference** *preference-value*] [**reject** | **blackhole**] **detect-group** *group-number*	Required

Auto Detect Implementation in VLAN Interface Backup

Using Auto Detect can help realize VLAN interfaces backup. When data can be transmitted through two VLAN interfaces on the device to the same destination, configure one of the VLAN interface as the active interface and the other as the standby interface. The standby interface is enabled automatically when the active fails, so as to ensure the data transmission. In this case, the Auto Detect function is implemented as follows:

- In normal situations (that is, when the detected group is **reachable**), the standby VLAN interface is down and packets are transmitted through the active VLAN interface.
- When the link between the active VLAN interface and the destination faults (that is, the detected group is **unreachable**), the system enables the backup VLAN interface.
- When the link between the active VLAN interface and the destination recovers (that is, the detected group becomes **reachable** again), the system shuts down the standby VLAN interface again.

Note

You need to create the detected group and perform configurations concerning VLAN interfaces before the following operations.

Follow these steps to configure the auto detect function for VLAN interface backup:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Enable the auto detect function to implement VLAN interface backup	**standby detect-group** *group-number*	Required This operation is only needed on the secondary VLAN interface.

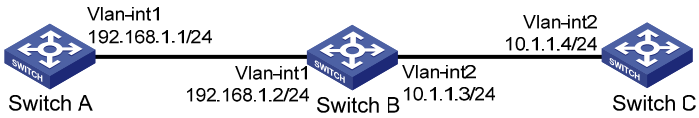
Auto Detect Configuration Examples

Configuration Example for Auto Detect Implementation in Static Routing

Network requirements

- As shown in Figure 1-1, create detected group 8 on Switch A; detect the reachability of the IP address 10.1.1.4, with 192.168.1.2 as the next hop, and the detecting number set to 1.
- On switch A, configure a static route to Switch C.
- Enable the static route when the detected group 8 is **reachable**.
- To ensure normal operating of the auto detect function, configure a static route to Switch A on Switch C.

Figure 1-1 Network diagram for implementing the auto detect function in static route



Configuration procedure

Configure the IP addresses of all the interfaces as shown in Figure 1-1. The configuration procedure is omitted.

- Configure Switch A.

Enter system view.

```
<SwitchA> system-view
```

Create detected group 8.

```
[SwitchA] detect-group 8
```

Detect the reachability of 10.1.1.4/24, with 192.168.1.2/24 as the next hop, and the detecting number set to 1.

```
[SwitchA-detect-group-8] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
[SwitchA-detect-group-8] quit
```

Enable the static route when the detected group is reachable. The static route is invalid when the detected group is unreachable.

```
[SwitchA] ip route-static 10.1.1.4 24 192.168.1.2 detect-group 8
```

- Configure Switch C.

Enter system view.

```
<SwitchC> system-view
```

Configure a static route to Switch A.

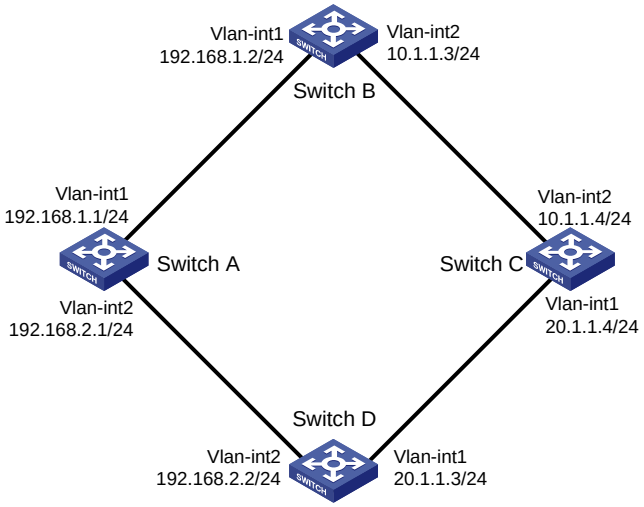
```
[SwitchC] ip route-static 192.168.1.1 24 10.1.1.3
```

Configuration Example for Auto Detect Implementation in VLAN Interface Backup

Network requirements

- As shown in Figure 1-2, make sure the routes between Switch A, Switch B, and Switch C, and between Switch A, Switch D, and Switch C are reachable.
- Create detected group 10 on Switch A to detect the connectivity between Switch B and Switch C.
- Configure VLAN-interface 1 to be the active interface, which is enabled when the detected group 10 is **reachable**.
- Configure VLAN-interface 2 to be the standby interface, which is enabled when the detected group 10 is **unreachable**.

Figure 1-2 Network diagram for VLAN interface backup



Configuration procedure

Configure the IP addresses of all the interfaces as shown in Figure 1-2. The configuration procedure is omitted.

Enter system view.

```
<SwitchA> system-view
```

Create auto detected group 10.

```
[SwitchA] detect-group 10
```

Add the IP address of 10.1.1.4 to detected group 10 to detect the reachability of the IP address, with the IP address of 192.168.1.2 as the next hop, and the detecting number set to 1.

```
[SwitchA-detect-group-10] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
[SwitchA-detect-group-10] quit
```

Specify to enable VLAN-interface 2 when the result of detected group 10 is **unreachable**.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] standby detect-group 10
```

Table of Contents

1 Voice VLAN Configuration 1-1
Voice VLAN Overview 1-1
How an IP Phone Works 1-1
How the Device Identifies Voice Traffic 1-3
Configuring Operation Mode for Voice VLAN 1-3
Support for Voice VLAN on Various Ports 1-4
Security Mode of Voice VLAN 1-5
Voice VLAN Configuration 1-6
Configuration Prerequisites 1-6
Configuring a Voice VLAN to Operate in Automatic Mode 1-6
Configuring a Voice VLAN to Operate in Manual Mode 1-7
Displaying and Maintaining Voice VLAN 1-9
Voice VLAN Configuration Example 1-9
Voice VLAN Configuration Example (Automatic Mode) 1-9
Voice VLAN Configuration Example (Manual Mode) 1-10

1 Voice VLAN Configuration

Note

The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Voice VLAN Overview

Voice VLANs are VLANs configured specially for voice traffic. By adding the ports connected with voice devices to voice VLANs, you can have voice traffic transmitted within voice VLANs and perform QoS-related configuration for voice traffic as required, thus ensuring the transmission priority of voice traffic and voice quality.

How an IP Phone Works

IP phones can convert analog voice signals into digital signals to enable them to be transmitted in IP-based networks. Used in conjunction with other voice devices, IP phones can offer large-capacity and low-cost voice communication solutions. As network devices, IP phones need IP addresses to operate properly in a network. Normally, an IP telephone automatically acquires an IP address from a DHCP server in its network.

When an IP phone applies for an IP address from a DHCP server, the IP phone can also apply for the following extensive information from the DHCP server through the Option184 field:

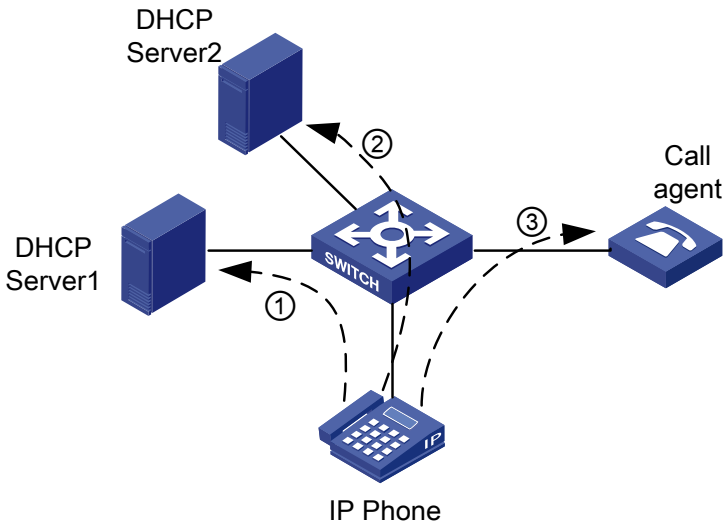
- IP address of the network call processor (NCP)
- IP address of the secondary NCP server
- Voice VLAN configuration
- Failover call routing

Note

The following contents just describe the IP address acquiring process of IP phones in general. Different IP phones may work differently. Refer to the IP Phones User Manual for details.

Following describes the way an IP phone acquires an IP address.

Figure 1-1 Network diagram for IP phones



As shown in Figure 1-1, the IP phone needs to work in conjunction with the DHCP server and the NCP to establish a path for voice data transmission. An IP phone goes through the following three phases to become capable of transmitting voice data.

1) After the IP phone is powered on, it sends an untagged DHCP request message containing four special requests in the Option 184 field besides the request for an IP address. The message is broadcast in the default VLAN of the receiving port. After receiving the DHCP request message, DHCP Server1, which resides in the default VLAN of the port receiving the message, responds as follows:

- If DHCP Server1 does not support Option 184, it returns the IP address assigned to the IP phone but ignores the other four special requests in the Option 184 field. Without information about voice VLAN, the IP phone can only send untagged packets in the default VLAN of the port the IP phone is connected to. In this case, you need to manually configure the default VLAN of the port as a voice VLAN.

Note

In cases where an IP phone obtains an IP address from a DHCP server that does not support Option 184, the IP phone directly communicates through the gateway after it obtains an IP address. It does not go through step 2 and step 3 described below.

- If DHCP Server1 supports Option 184, it returns the IP address assigned to the IP phone, the IP address of the NCP, the voice VLAN ID, and so on.

2) On acquiring the voice VLAN ID from DHCP Server1, the IP phone ignores the IP address assigned by DHCP Server1 and sends a new DHCP request message carrying the voice VLAN tag to the voice VLAN. After receiving the DHCP request, DHCP Server2 residing in the voice VLAN assigns a new IP address to the IP phone and sends a tagged response message to the IP phone. After the IP phone receives the tagged response message, it sends voice data packets tagged with the voice VLAN tag. In this case, the port on the device connecting to the IP phone must be configured to allow packets tagged with the voice VLAN tag to pass.

3) After the IP phone acquires the IP address assigned by DHCP Server2, the IP phone establishes a connection to the NCP specified by DHCP Server1 and downloads corresponding software. After that, the IP phone can communicate properly.



Note

- An untagged packet carries no VLAN tag.
- A tagged packet carries the tag of a VLAN.

How the Device Identifies Voice Traffic

The device determines whether a received packet is a voice packet by checking its source MAC address. Packets with their source MAC addresses complying with the configured OUI (organizationally unique identifier) addresses are treated as voice packets. Ports receiving packets of this type will be added to the voice VLAN automatically for transmitting voice data.

You can configure OUI addresses for voice packets or specify to use the default OUI addresses.



Note

An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address. The WX3000 supports OUI address mask configuration. You can adjust the matching depth of MAC address by setting different OUI address masks.

The following table lists the five default OUI addresses on the device.

Table 1-1 Default OUI addresses preset on the device

Number	OUI address	Vendor
1	0003-6b00-0000	Cisco phones
2	000f-e200-0000	H3C Aolynk phones
3	00d0-1e00-0000	Pingtel phones
4	00e0-7500-0000	Polycom phones
5	00e0-bb00-0000	3Com phones

Configuring Operation Mode for Voice VLAN

A voice VLAN can operate in two modes: automatic and manual. You can configure the operation mode for the voice VLAN according to data traffic passing through a port.

Processing mode of untagged packets sent by IP voice devices

- Automatic mode. A WX3000 device automatically adds a port connecting an IP voice device to the voice VLAN by learning the source MAC address in the untagged packet sent by the IP voice device when it is powered on. The voice VLAN uses the aging mechanism to maintain the number of ports in the voice VLAN. When the aging timer expires, the ports whose OUI addresses are not updated (that is, no voice traffic passes) will be removed from the voice VLAN. In automatic mode, ports can not be added to or removed from a voice VLAN manually.
- Manual mode: In this mode, you need to add a port to a voice VLAN or remove a port from a voice VLAN manually.

Processing mode of tagged packets sent by IP voice devices

Tagged packets from IP voice devices are forwarded based on their tagged VLAN IDs, whether the automatic or manual mode is used.

Caution

- If the voice traffic transmitted by an IP voice device carries VLAN tags, and 802.1x authentication and guest VLAN is enabled on the port which the IP voice device is connected to, assign different VLAN IDs for the voice VLAN, the default VLAN of the port, and the 802.1x guest VLAN to ensure the effective operation of these functions.
- If the voice traffic transmitted by an IP voice device carries no VLAN tag, the default VLAN of the port which the IP voice device is connected to must be configured as the voice VLAN. In this case, the 802.1x authentication is unavailable.

Support for Voice VLAN on Various Ports

Voice VLAN packets can be forwarded by access ports, trunk ports, and hybrid ports. You can enable a trunk or hybrid port belonging to other VLANs to forward voice and service packets simultaneously by enabling the voice VLAN.

The support for different types of voice traffic (that is, tagged traffic and untagged traffic) varies with port mode and port type, as listed in Table 1-2.

Table 1-2 Matching relationship between port types and voice traffic types

Port voice VLAN mode	Voice traffic type	Port type	Supported or not
Automatic mode	Tagged voice traffic	Access	Not supported
		Trunk	Supported Make sure the default VLAN of the port exists and is not a voice VLAN. And the access port permits the traffic of the default VLAN.
		Hybrid	Supported Make sure the default VLAN of the port exists and is not a voice VLAN. The default VLAN must be in the list of the tagged VLANs whose traffic is permitted by the access port.
	Untagged voice traffic	Access	Not supported, because the default VLAN of the port must be a voice VLAN and the access port is in the voice VLAN. This can be done by adding the port to the voice VLAN manually.
		Trunk	
		Hybrid	
Manual mode	Tagged voice traffic	Access	Not supported
		Trunk	Supported Make sure the default VLAN of the port exists and is not a voice VLAN. And the access port permits the traffic of the default VLAN.
		Hybrid	Supported Make sure the default VLAN of the port exists and is in the list of the tagged VLANs whose traffic is permitted by the access port.
	Untagged voice traffic	Access	Supported Make sure the default VLAN of the port is a voice VLAN.
		Trunk	Supported Make sure the default VLAN of the port is a voice VLAN and the port permits the traffic of the VLAN.
		Hybrid	Supported Make sure the default VLAN of the port is a voice VLAN and is in the list of untagged VLANs whose traffic is permitted by the port.

Security Mode of Voice VLAN

On the WX3000 devices, a voice VLAN can operate in the security mode. Voice VLANs operating in this mode only permit voice data, enabling you to perform voice traffic-specific priority configuration. With the security mode disabled, both voice data and service data can be transmitted in a voice VLAN.

Voice VLAN Configuration

Configuration Prerequisites

- Create the corresponding VLAN before configuring a voice VLAN.
- VLAN 1 (the default VLAN) cannot be configured as a voice VLAN.

Configuring a Voice VLAN to Operate in Automatic Mode

Follow these steps to configure a voice VLAN to operate in automatic mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set an OUI address that can be identified by the voice VLAN	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	Optional By default, the device determines the voice traffic according to the default OUI address.
Enable the voice VLAN security mode	**voice vlan security enable**	Optional By default, the voice VLAN security mode is enabled.
Set the aging time for the voice VLAN	**voice vlan aging** *minutes*	Optional The default aging time is 1,440 minutes.
Enable the voice VLAN function globally	**voice vlan** *vlan-id* **enable**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	Required
Enable the voice VLAN function on a port	**voice vlan enable**	Required By default, voice VLAN is disabled.
Enable the voice VLAN legacy function on the port	**voice vlan legacy**	Optional By default, voice VLAN legacy is disabled.
Set the voice VLAN operation mode on a port to automatic.	**voice vlan mode auto**	Optional The default voice VLAN operation mode on a port is automatic.

Caution

- For a voice VLAN operating in automatic mode, it does not support the adding of an Access port, and thus a voice VLAN cannot function when configuring with the VLAN VPN function.
- For a voice VLAN operating in automatic mode, it only supports that the Hybrid port to process the tagged voice traffic. However, the protocol VLAN feature requires the Hybrid port to remove tags from the packets, see the VLAN part of this manual for details. Therefore, a VLAN cannot be configured as a voice VLAN and a protocol VLAN simultaneously.
- For a port operating in automatic mode, a default VLAN cannot be configured as a voice VLAN; otherwise the system prompts you for unsuccessful configuration.

Note

When the voice VLAN is working normally, if the device restarts, in order to make the established voice connections work normally, the system does not need to be triggered by the voice traffic to add the port in automatic mode to the local devices of the voice VLAN but does so immediately after the restart.

Configuring a Voice VLAN to Operate in Manual Mode

Follow these steps to configure a voice VLAN to operate in manual mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set an OUI address that can be identified by the voice VLAN	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	Optional Without this address, the default OUI address is used.
Enable the voice VLAN security mode	**voice vlan security enable**	Optional By default, the voice VLAN security mode is enabled.
Set the aging time for a voice VLAN	**voice vlan aging** *minutes*	Optional The default aging time is 1,440 minutes.
Enable the voice VLAN function globally	**voice vlan** *vlan-id* **enable**	Required
Enter port view	**interface** *interface-type interface-number*	Required
Enable voice VLAN on a port	**voice vlan enable**	Required By default, voice VLAN is disabled on a port.
Enable the voice VLAN legacy function on the port	**voice vlan legacy**	Optional By default, voice VLAN legacy is disabled.
Set voice VLAN operation mode on a port to manual	**undo voice vlan mode auto**	Required The default voice VLAN operation mode on a port is automatic.
Quit to system view	**quit**	—

To do…			Use the command…	Remarks
Add a port in manual mode to the voice VLAN	Access port	Enter VLAN view	**vlan** *vlan-id*	Required By default, all the ports belong to VLAN 1.
		Add the port to the VLAN	**port** *interface-list*	
	Trunk or Hybrid port	Enter port view	**interface** *interface-type interface-num*	
		Add the port to the VLAN	**port trunk permit vlan** *vlan-id* **port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	
		Configure the voice VLAN to be the default VLAN of the port	**port trunk pvid vlan** *vlan-id* **port hybrid pvid vlan** *vlan-id*	Optional Refer to Table 1-2 to determine whether or not this operation is needed.

Caution

- The voice VLAN function can be enabled for only one VLAN at one time.
- If the Link Aggregation Control Protocol (LACP) is enabled on a port, voice VLAN feature cannot be enabled on it.
- Voice VLAN function can be enabled only for the static VLAN. A dynamic VLAN cannot be configured as a voice VLAN.
- When ACL number applied to a port reaches to its threshold, voice VLAN cannot be enabled on this port. You can use the **display voice vlan error-info** command to locate such ports.
- When a voice VLAN operates in security mode, the device in it permits only the packets whose source addresses are the identified voice OUI addresses. Packets whose source addresses cannot be identified, including certain authentication packets (such as 802.1x authentication packets), will be dropped. Therefore, you are suggested not to transmit both voice data and service data in a voice VLAN. If you have to do so, make sure that the voice VLAN does not operate in security mode.
- The voice VLAN legacy feature realizes the communication between the WX3000 series devices and other vendor's voice devices by automatically adding the voice VLAN tag to the voice data coming from other vendors' voice device. The **voice vlan legacy** command can be executed before voice VLAN is enabled globally and on a port, but it takes effect only after voice VLAN is enabled globally and on the port.

Note

To add a Trunk port or a Hybrid port to the voice VLAN, refer to *Basic Port Configurations* of the *3Com WX3000 Series Unified Switches Switching Engines Command Manual* for the related command.

Displaying and Maintaining Voice VLAN

To do…	Use the command…	Remarks
Display the information about ports on which voice VLAN configuration fails	**display voice vlan error-info**	You can execute the **display** command in any view.
Display the voice VLAN configuration status	**display voice vlan status**	
Display the currently valid OUI addresses	**display voice vlan oui**	
Display the ports operating in the current voice VLAN	**display vlan** *vlan-id*	

Voice VLAN Configuration Example

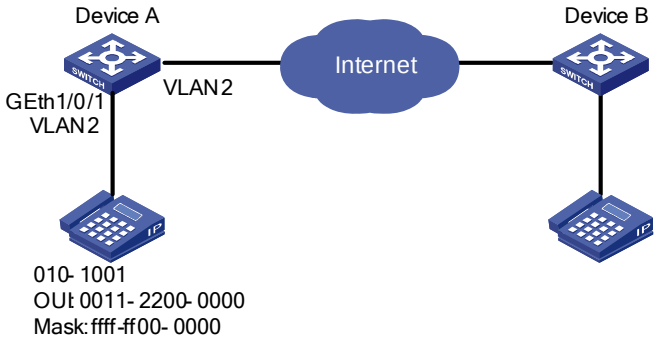
Voice VLAN Configuration Example (Automatic Mode)

Network requirements

Create a voice VLAN and configure it to operate in automatic mode to enable the port to which an IP phone is connected to join or exit the voice VLAN automatically and voice traffic to be transmitted within the voice VLAN, as shown in Figure 1-2.

- Create VLAN 2 and configure it as a voice VLAN, with the aging time being 100 minutes.
- The IP phone sends tagged packets. It is connected to GigabitEthernet 1/0/1, a hybrid port, with VLAN 6 being its default VLAN. Set this port to operate in automatic mode.
- You need to add a user-defined OUI address 0011-2200-000, with the mask being ffff-ff00-0000 and the description string being “test”.

Figure 1-2 Network diagram for voice VLAN configuration (automatic mode)



Configuration procedure

Create VLAN 2 and VLAN 6.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] vlan 6
[DeviceA-vlan6] quit
```

Set the aging time for the voice VLAN.

```
[DeviceA] voice vlan aging 100
```

Add a user-defined OUI address 0011-2200-000 and set the description string to “test”.

```
[DeviceA] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 description test
```

Enable the voice VLAN function globally.

```
[DeviceA] voice vlan 2 enable
```

Configure the vocie VLAN to operate in automatic mode on GigabitEthernet 1/0/1. This operation is optional. By default, a voice VLAN operates in automatic mode on a port.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] voice vlan mode auto
```

Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

Configure VLAN 6 as the default VLAN of GigabitEthernet 1/0/1, and configure GigabitEthernet 1/0/1 to permit packets with the tag of VLAN 6.

```
[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 6
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 6 tagged
```

Enable the voice VLAN function on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] voice vlan enable
```

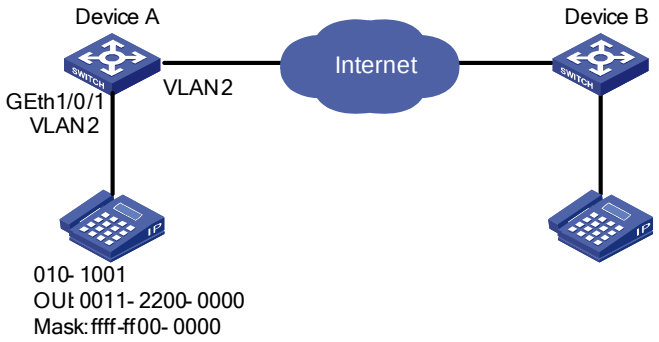
Voice VLAN Configuration Example (Manual Mode)

Network requirements

Create a voice VLAN and configure it to operate in manual mode. Add the port to which an IP phone is connected to the voice VLAN to enable voice traffic to be transmitted within the voice VLAN, as shown in Figure 1-3.

- Create VLAN 2 and configure it as a voice VLAN. Set the voice VLAN to operate in security mode
- The IP phone sends untagged packets. It is connected to GigabitEthernet 1/0/1, a hybrid port. Set this port to operate in manual mode.
- You need to add a user-defined OUI address 0011-2200-000, with the mask being ffff-ff00-0000 and the description string being “test”.

Figure 1-3 Network diagram for voice VLAN configuration (manual mode)



Configuration procedure

Enable the security mode for the voice VLAN so that the ports in the voice VLAN permit valid voice packets only. This operation is optional. The security mode is enabled by default.

```
<DeviceA> system-view
[DeviceA] voice vlan security enable
```

Add a user-defined OUI address 0011-2200-000 and set the description string to “test”.

```
[DeviceA] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 description test
```

Create VLAN 2 and configure it as a voice VLAN.

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] voice vlan 2 enable
```

Configure GigabitEthernet 1/0/1 to operate in manual mode.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo voice vlan mode auto
```

Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

Configure the voice VLAN as the default VLAN of GigabitEthernet 1/0/1, and add the voice VLAN to the list of untagged VLANs whose traffic is permitted by the port.

```
[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 2
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
```

Enable the voice VLAN function on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] voice vlan enable
```

Verification

Display the OUI addresses, the corresponding OUI address masks and the corresponding description strings that the system supports.

```
<DeviceA> display voice vlan oui
Oui Address     Mask            Description
0003-6b00-0000  ffff-ff00-0000  Cisco phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0011-2200-0000  ffff-ff00-0000  test
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

Display the status of the current voice VLAN.

```
<DeviceA> display voice vlan status
Voice Vlan status: ENABLE
Voice Vlan ID: 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1440 minutes
Current voice vlan enabled port mode:
PORT                    MODE
----------------------------------------
GigabitEthernet1/0/1           MANUAL
```

Table of Contents

1 GVRP Configuration 1-1
Introduction to GVRP 1-1
GARP 1-1
GVRP 1-4
Protocol Specifications 1-4
GVRP Configuration 1-4
Configuration Task List 1-4
Enabling GVRP 1-4
Configuring GVRP Timers 1-5
Configuring GVRP Port Registration Mode 1-6
Displaying and Maintaining GVRP 1-6
GVRP Configuration Example 1-7
GVRP Configuration Example 1-7

1 GVRP Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Introduction to GVRP

GARP VLAN registration protocol (GVRP) is an implementation of generic attribute registration protocol (GARP). GARP is introduced as follows.

GARP

The generic attribute registration protocol (GARP), provides a mechanism that allows participants in a GARP application to distribute, propagate, and register with other participants in a bridged LAN the attributes specific to the GARP application, such as the VLAN or multicast attribute.

GARP itself does not exist on a device as an entity. GARP-compliant application entities are called GARP applications. One example is GVRP. When a GARP application entity is present on a port on your device, this port is regarded a GARP application entity.

GARP messages and timers

1) GARP messages

GARP members communicate with each other through the messages exchanged between them. The messages performing important functions for GARP fall into three types: Join, Leave and LeaveAll.

- When a GARP entity wants its attribute information to be registered on other devices, it sends Join messages to these devices. A GARP entity also sends Join messages when it receives Join messages from other entities or it wants some of its statically configured attributes to be registered on other GARP entities.
- When a GARP entity wants some of its attributes to be deregistered on other devices, it sends Leave messages to these devices. A GARP entity also sends Leave messages when it receives Leave messages from other entities for deregistering some attributes or it has some attributes statically deregistered.
- Once a GARP entity is launched, the LeaveAll timer is triggered at the same time. The GARP entity sends out LeaveAll messages after the timer times out. LeaveAll messages deregister all the attributes, through which the attribute information of the entity can be registered again on the other GARP entities.

Leave messages, LeaveAll messages, together with Join messages ensure attribute information can be deregistered and re-registered.

Through message exchange, all the attribute information to be registered can be propagated to all the GARP-enabled switches in the same LAN.

2) GARP timers

Timers determine the intervals of sending different types of GARP messages. GARP defines four timers to control the period of sending GARP messages.

- Hold: When a GARP entity receives a piece of registration information, it does not send out a Join message immediately. Instead, to save the bandwidth resources, it starts the Hold timer and puts all received registration information before the timer times out into one Join message and sends out the message after the timer times out.
- Join: To make sure the devices can receive Join messages, each Join message is sent twice. If the first Join message sent is not responded for a specific period, a second one is sent. The period is determined by this timer.
- Leave: When a GARP entity expects to deregister a piece of attribute information, it sends out a Leave message. Any GARP entity receiving this message starts its Leave timer, and deregisters the attribute information if it does not receives a Join message again before the timer times out.
- LeaveAll: Once a GARP entity starts up, it starts the LeaveAll timer, and sends out a LeaveALL message after the timer times out, so that other GARP entities can re-register all the attribute information on this entity. After that, the entity restarts the LeaveAll timer to begin a new cycle.

Note

- The settings of GARP timers apply to all GARP applications, such as GVRP, on a LAN.
- Unlike other three timers, which are set on a port basis, the LeaveAll timer is set in system view and takes effect globally.
- A GARP application entity may send LeaveAll messages at the interval set by its LeaveAll timer or the LeaveAll timer on another device on the network, whichever is smaller. This is because each time a device on the network receives a LeaveAll message it resets its LeaveAll timer.

Operating mechanism of GARP

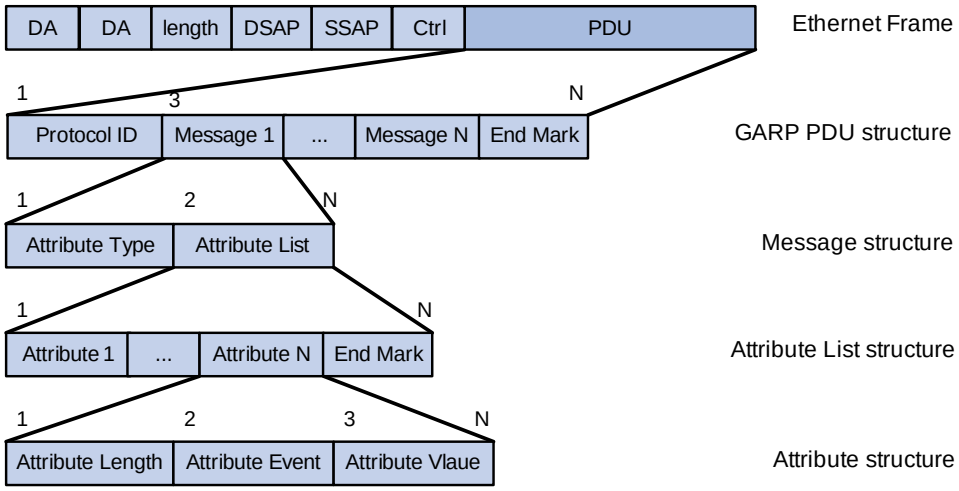
Through the mechanism of GARP, the configuration information on a GARP member will be propagated within the whole LAN. A GARP member can be a terminal workstation or a bridge; it instructs other GARP members to register/deregister its attribute information by declaration/recant, and register/deregister other GARP member's attribute information according to other member's declaration/recant. When a port receives an attribute declaration, the port will register this attribute. When a port receives an attribute recant, the port will deregister this attribute.

The protocol packets of GARP entities use specific multicast MAC addresses as their destination MAC addresses. When receiving these packets, the switch distinguishes them by their destination MAC addresses and delivers them to different GARP application (for example, GVRP) for further processing.

GARP message format

The GARP packets are in the following format:

Figure 1-1 Format of GARP packets



The following table describes the fields of a GARP packet.

Table 1-1 Description of GARP packet fields

Field	Description	Value
Protocol ID	Protocol ID	1
Message	Each message consists of two parts: Attribute Type and Attribute List.	—
Attribute Type	Defined by the specific GARP application	The attribute type of GVRP is 0x01.
Attribute List	It contains multiple attributes.	—
Attribute	Each general attribute consists of three parts: Attribute Length, Attribute Event, and Attribute Value. Each LeaveAll attribute consists of two parts: Attribute Length and LeaveAll Event.	—
Attribute Length	The length of the attribute	2 to 255 (in bytes)
Attribute Event	The event described by the attribute	0: LeaveAll Event 1: JoinEmpty 2: JoinIn 3: LeaveEmpty 4: LeaveIn 5: Empty
Attribute Value	The value of the attribute	For GVRP packets, the value of this field is the VLAN ID; however, for LeaveAll messages, this field is invalid.
End Mark	End mark of an GARP PDU	The value of this field is fixed to 0x00.

GVRP

As an implementation of GARP, GARP VLAN registration protocol (GVRP) maintains dynamic VLAN registration information and propagates the information to the other devices through GARP.

With GVRP enabled on a device, the VLAN registration information received by the device from other devices is used to dynamically update the local VLAN registration information, including the information about the VLAN members, the ports through which the VLAN members can be reached, and so on. The device also propagates the local VLAN registration information to other devices so that all the devices in the same LAN can have the same VLAN information. VLAN registration information propagated by GVRP includes static VLAN registration information, which is manually configured locally on each device, and dynamic VLAN registration information, which is received from other devices.

GVRP has the following three port registration modes: Normal, Fixed, and Forbidden, as described in the following.

- Normal. A port in this mode can dynamically register/deregister VLANs and propagate dynamic/static VLAN information.
- Fixed. A port in this mode cannot register/deregister VLANs dynamically. It only propagates static VLAN information. Besides, the port permits only static VLANs, that is, it propagates only static VLAN information to the other GARP members.
- Forbidden. A port in this mode cannot register/deregister VLANs dynamically. It permits only the default VLAN (namely, VLAN 1), that is, the port propagates only the information about VLAN 1 to the other GARP members.

Protocol Specifications

GVRP is defined in IEEE 802.1Q standard.

GVRP Configuration

Configuration Task List

Complete the following tasks to configure GVRP:

Task	Remarks
Enabling GVRP	Required
Configuring GVRP Timers	Optional
Configuring GVRP Port Registration Mode	Optional

Enabling GVRP

Configuration Prerequisite

The port on which GVRP will be enabled must be set to a trunk port.

Configuration procedure

Follow these steps to enable GVRP on an Ethernet port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable GVRP globally	**gvrp**	Required By default, GVRP is disabled globally.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable GVRP on the port	**gvrp**	Required By default, GVRP is disabled on the port.

Note

After you enable GVRP on a trunk port, you cannot change the port to a different type.

Configuring GVRP Timers

Follow these steps to configure GVRP timers:

To do…	Use the command…	Remarks
Enter system view	system-view	—
Configure the LeaveAll timer	**garp timer leaveall** *timer-value*	Optional By default, the LeaveAll timer is set to 1,000 centiseconds.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the Hold, Join, and Leave timers	**garp timer** { **hold** | **join** | **leave** } *timer-value*	Optional By default, the Hold, Join, and Leave timers are set to 10, 20, and 60 centiseconds respectively.

Note that:

- The setting of each timer must be a multiple of 5 (in centiseconds).
- The timeout ranges of the timers vary depending on the timeout values you set for other timers. If you want to set the timeout time of a timer to a value out of the current range, you can set the timeout time of the associated timer to another value to change the timeout range of this timer.

The following table describes the relations between the timers:

Table 1-2 Relations between the timers

Timer	Lower threshold	Upper threshold
Hold	10 centiseconds	This upper threshold is less than or equal to one-half of the timeout time of the Join timer. You can change the threshold by changing the timeout time of the Join timer.
Join	This lower threshold is greater than or equal to twice the timeout time of the Hold timer. You can change the threshold by changing the timeout time of the Hold timer.	This upper threshold is less than one-half of the timeout time of the Leave timer. You can change the threshold by changing the timeout time of the Leave timer.
Leave	This lower threshold is greater than twice the timeout time of the Join timer. You can change the threshold by changing the timeout time of the Join timer.	This upper threshold is less than the timeout time of the LeaveAll timer. You can change the threshold by changing the timeout time of the LeaveAll timer.
LeaveAll	This lower threshold is greater than the timeout time of the Leave timer. You can change threshold by changing the timeout time of the Leave timer.	32,765 centiseconds

Configuring GVRP Port Registration Mode

Follow these steps to configure GVRP port registration mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure GVRP port registration mode	**gvrp registration** { **fixed** | **forbidden** | **normal** }	Optional By default, GVRP port registration mode is normal.

Displaying and Maintaining GVRP

To do…	Use the command…	Remarks
Display GARP statistics	**display garp statistics** [**interface** *interface-list*]	You can execute the **display** command in any view.
Display the settings of the GARP timers	**display garp timer** [**interface** *interface-list*]	
Display GVRP statistics	**display gvrp statistics** [**interface** *interface-list*]	
Display the global GVRP status	**display gvrp status**	
Clear GARP statistics	**reset garp statistics** [**interface** *interface-list*]	You can execute the **reset** command in user view

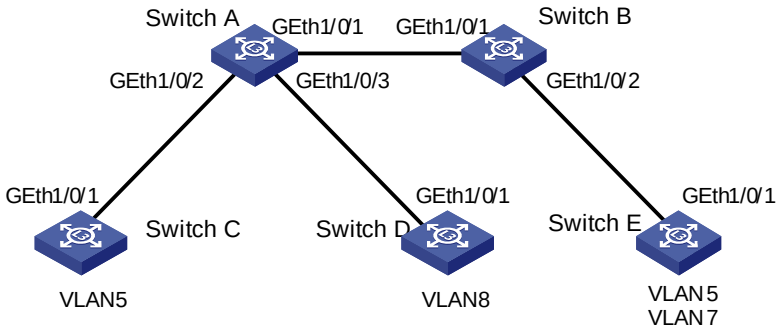
GVRP Configuration Example

GVRP Configuration Example

Network requirements

- Enable GVRP on all the switches in the network so that the VLAN configurations on Switch C and Switch E can be applied to all switches in the network, thus implementing dynamic VLAN information registration and refresh, as shown in Figure 1-2.
- By configuring the GVRP registration modes of specific Ethernet ports, you can enable the corresponding VLANs in the switched network to communicate with each other.

Figure 1-2 Network diagram for GVRP configuration



Configuration procedure

1) Configure Switch A

Enable GVRP globally.

```
<SwitchA> system-view
[SwitchA] gvrp
```

Configure GigabitEthernet 1/0/1 to be a trunk port and to permit the packets of all the VLANs.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable GVRP on GigabitEthernet 1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] gvrp
[SwitchA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 to be a trunk port and to permit the packets of all the VLANs.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan all
```

Enable GVRP on GigabitEthernet 1/0/2.

```
[SwitchA-GigabitEthernet1/0/2] gvrp
[SwitchA-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 to be a trunk port and to permit the packets of all the VLANs.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
```

```
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan all
```

Enable GVRP on GigabitEthernet 1/0/3.

```
[SwitchA-GigabitEthernet1/0/3] gvrp
[SwitchA-GigabitEthernet1/0/3] quit
```

2) Configure Switch B

The configuration procedure of Switch B is similar to that of Switch A and is thus omitted.

3) Configure Switch C

Enable GVRP on Switch C, which is similar to that of Switch A and is thus omitted.

Create VLAN 5.

```
[SwitchC] vlan 5
[SwitchC-vlan5] quit
```

4) Configure Switch D

Enable GVRP on Switch D, which is similar to that of Switch A and is thus omitted.

Create VLAN 8.

```
[SwitchD] vlan 8
[SwitchD-vlan8] quit
```

5) Configure Switch E

Enable GVRP on Switch E, which is similar to that of Switch A and is thus omitted.

Create VLAN 5 and VLAN 7.

```
[SwitchE] vlan 5
[SwitchE-vlan5] quit
[SwitchE] vlan 7
[SwitchE-vlan7] quit
```

6) Display the VLAN information dynamically registered on Switch A, Switch B, and Switch E.

Display the VLAN information dynamically registered on Switch A.

```
[SwitchA] display vlan dynamic
 Total 3 dynamic VLAN exist(s).
 The following dynamic VLANs exist:
  5, 7, 8,
```

Display the VLAN information dynamically registered on Switch B.

```
[SwitchB] display vlan dynamic
 Total 3 dynamic VLAN exist(s).
 The following dynamic VLANs exist:
  5, 7, 8,
```

Display the VLAN information dynamically registered on Switch E.

```
[SwitchE] display vlan dynamic
 Total 1 dynamic VLAN exist(s).
 The following dynamic VLANs exist:
  8
```

7) Configure GigabitEthernet 1/0/1 on Switch E to operate in fixed GVRP registration mode and display the VLAN information dynamically registered on Switch A, Switch B, and Switch E.

Configure GigabitEthernet 1/0/1 on Switch E to operate in fixed GVRP registration mode.

```
[SwitchE] interface GigabitEthernet 1/0/1
```

```
[SwitchE-GigabitEthernet1/0/1] gvrp registration fixed
```

Display the VLAN information dynamically registered on Switch A.

```
[SwitchA] display vlan dynamic
 Total 3 dynamic VLAN exist(s).
 The following dynamic VLANs exist:
  5, 7, 8,
```

Display the VLAN information dynamically registered on Switch B.

```
[SwitchB] display vlan dynamic
 Total 3 dynamic VLAN exist(s).
 The following dynamic VLANs exist:
  5, 7, 8,
```

Display the VLAN information dynamically registered on Switch E.

```
[SwitchE-GigabitEthernet1/0/1] display vlan dynamic
  No dynamic vlans exist!
```

8) Configure GigabitEthernet 1/0/1 on Switch E to operate in forbidden GVRP registration mode and display the VLAN registration information dynamically registered on Switch A, Switch B, and Switch E.

Configure GigabitEthernet 1/0/1 on Switch E to operate in forbidden GVRP registration mode.

```
[SwitchE-GigabitEthernet1/0/1] gvrp registration forbidden
```

Display the VLAN information dynamically registered on Switch A.

```
[SwitchA] display vlan dynamic
 Total 2 dynamic VLAN exist(s).
 The following dynamic VLANs exist:
  5, 8,
```

Display the VLAN information dynamically registered on Switch B.

```
[SwitchB] display vlan dynamic
 Total 2 dynamic VLAN exist(s).
 The following dynamic VLANs exist:
  5, 8,
```

Display the VLAN information dynamically registered on Switch E.

```
[SwitchE] display vlan dynamic
  No dynamic vlans exist!
```

Table of Contents

1 Basic Port Configuration ····· 1-1
Ethernet Port Overview ····· 1-1
Types and Numbers of Ethernet Ports ····· 1-1
Combo Ports Mapping Relations ····· 1-1
Link Types of Ethernet Ports ····· 1-2
Configuring the Default VLAN ID for an Ethernet Port ····· 1-2
Adding an Ethernet Port to Specified VLANs ····· 1-3
Configuring Ethernet Ports ····· 1-3
Making Basic Port Configuration ····· 1-3
Configuring Port Auto-Negotiation Speed ····· 1-4
Setting the Ethernet Port Broadcast Suppression Ratio ····· 1-5
Enabling Flow Control on a Port ····· 1-5
Configuring Access Port Attribute ····· 1-6
Configuring Hybrid Port Attribute ····· 1-6
Configuring Trunk Port Attribute ····· 1-6
Disabling Up/Down Log Output on a Port ····· 1-7
Copying Port Configuration to Other Ports ····· 1-8
Configuring a Port Group ····· 1-8
Setting Loopback Detection for an Ethernet Port ····· 1-9
Configuring the Ethernet Port to Run Loopback Test ····· 1-10
Enabling the System to Test Connected Cable ····· 1-11
Configuring the Interval to Perform Statistical Analysis on Port Traffic ····· 1-11
Displaying and Maintaining Ethernet Ports ····· 1-12
Ethernet Port Configuration Example ····· 1-12
Troubleshooting Ethernet Port Configuration ····· 1-13

1 Basic Port Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Ethernet Port Overview

Types and Numbers of Ethernet Ports

Table 1-1 lists the types and numbers of the Ethernet ports available on the WX3000 series devices.

Table 1-1 Description of Ethernet port type and port number

Series	10/100/1000Base-T autosensing Ethernet ports	1000Base-X SFP ports	Extension slots
WX3024	24	4	2
WX3010	8	2	None
WX3008	8	None	None

Combo Ports Mapping Relations

An SFP port and its corresponding 10/100/1000Base-T autosensing Ethernet port form a Combo port. That is, only one of the two ports forming the Combo port can be used at a time. Table 1-2 shows the mapping relations between the ports forming the Combo port.

Table 1-2 Mapping relations between the ports forming the Combo port

Series	1000Base-X SFP port	10/100/1000Base-T autosensing Ethernet port
WX3024	GigabitEthernet 1/0/25	GigabitEthernet 1/0/22
	GigabitEthernet 1/0/26	GigabitEthernet 1/0/24
	GigabitEthernet 1/0/27	GigabitEthernet 1/0/21
	GigabitEthernet 1/0/28	GigabitEthernet 1/0/23

Link Types of Ethernet Ports

An Ethernet port of the device can operate in one of the following three link types:

- Access: An access port can belong to only one VLAN, and is generally used to connect user PCs.
- Trunk: A trunk port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs, and is generally used to connect another device.
- Hybrid: A hybrid port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs, and can be used to connect either a device or user PC.



Note

A hybrid port allows the packets of multiple VLANs to be sent without tags, but a trunk port only allows the packets of the default VLAN to be sent without tags.

You can configure all the three types of ports on the same Ethernet switch. However, note that you cannot directly switch a port between trunk and hybrid and you must set the port as access before the switching. For example, to change a trunk port to hybrid, you must first set it as access and then hybrid.

Configuring the Default VLAN ID for an Ethernet Port

An access port can belong to only one VLAN. Therefore, the VLAN an access port belongs to is also the default VLAN of the access port. A hybrid/trunk port can belong to several VLANs, and so a default VLAN ID for the port is required.

- After you configure default VLAN IDs for Ethernet ports, the packets passing through the ports are processed in different ways depending on different situations:

Table 1-3 Processing of incoming/outgoing packets

<table>
<tr><th rowspan="2">Port type</th><th colspan="2">Processing of an incoming packet</th><th rowspan="2">Processing of an outgoing packet</th></tr>
<tr><th>If the packet does not carry a VLAN tag</th><th>If the packet carries a VLAN tag</th></tr>
<tr><td>Access</td><td rowspan="3">Receive the packet and add the default tag to the packet.</td><td>• If the VLAN ID is just the default VLAN ID, receive the packet.
• If the VLAN ID is not the default VLAN ID, discard the packet.</td><td>Deprive the tag from the packet and send the packet.</td></tr>
<tr><td>Trunk</td><td rowspan="2">• If the VLAN ID is just the default VLAN ID, receive the packet.
• If the VLAN ID is not the default VLAN ID but is one of the VLAN IDs allowed to pass through the port, receive the packet.
• If the VLAN ID is neither the default VLAN ID, nor one of the VLAN IDs allowed to pass through the port, discard the packet.</td><td>• If the VLAN ID is just the default VLAN ID, deprive the tag and send the packet.
• If the VLAN ID is not the default VLAN ID, keep the original tag unchanged and send the packet.</td></tr>
<tr><td>Hybrid</td><td>• If the VLAN ID is just the default VLAN ID, deprive the tag and send the packet.
• If the VLAN ID is not the default VLAN ID, deprive the tag or keep the tag unchanged (whichever is done is determined by the port hybrid vlan vlan-id-list { tagged | untagged } command) and send the packet.</td></tr>
</table>

Caution

To guarantee the proper packet forwarding, the default VLAN ID of the local hybrid port or trunk port should be identical with that of the hybrid port or trunk port on the peer device.

Adding an Ethernet Port to Specified VLANs

You can add the specified Ethernet port to a specified VLAN. After that, the Ethernet port can forward the packets of the specified VLAN, so that the VLAN on this switch can intercommunicate with the same VLAN on the peer device.

An access port can only be added to one VLAN, while hybrid and trunk ports can be added to multiple VLANs.

Note that the port shall be added to an existing VLAN.

Configuring Ethernet Ports

Making Basic Port Configuration

Follow these steps to make basic port configuration:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the Ethernet port	**undo shutdown**	By default, the port is enabled. Use the **shutdown** command to disable the port.
Set the description of the Ethernet port	**description** *text*	By default, no description is defined for an Ethernet port.
Set the duplex mode of the Ethernet port	**duplex** { **auto** | **full** | **half** }	The port defaults to **auto** (autonegotiation) mode.
Set the rate of the Ethernet port	**speed** { **10** | **100** | **1000** | **auto** }	By default, the speed of the port is set to **auto** mode.
Set the MDI attribute of the Ethernet port	**mdi** { **across** | **auto** | **normal** }	Be default, the MDI attribute of the port is set to **auto** mode.
Allow jumbo frames that are not larger than 4096 bytes to pass through the Ethernet port	**jumboframe enable**	Optional By default, jumbo frames that are not larger than 4096 bytes are allowed to pass through the port.

Note

- For a combo port, only after the optical interface has been configured with the **shutdown** command can the electrical interface be used, and vice versa.
- The **speed** and **mdi** commands are not available on the combo port.
- The **mdi** command is not available on the Ethernet ports of the expansion interface card.

Configuring Port Auto-Negotiation Speed

You can configure an auto-negotiation speed for a port by using the **speed auto** command.

Take a 10/100/1000 Mbps port as an example.

- If you expect that 10 Mbps is the only available auto-negotiation speed of the port, you just need to configure **speed auto 10**.
- If you expect that 10 Mbps and 100 Mbps are the available auto-negotiation speeds of the port, you just need to configure **speed auto 10 100**.
- If you expect that 10 Mbps and 1000 Mbps are the available auto-negotiation speeds of the port, you just need to configure **speed auto 10 1000**.

Follow these steps to configure auto-negotiation speeds for a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet interface view	**interface** *interface-type interface-number*	—

To do…	Use the command…	Remarks
Configure the available auto-negotiation speed(s) for the port	**speed auto** [**10** | **100** | **1000**]*	Optional By default, the port speed is auto-negotiated.



Note

- Only ports on the front panel of the device support the auto-negotiation speed configuration feature. And ports on the extended interface card do not support this feature currently.
- After you configure auto-negotiation speed(s) for a port, if you execute the **undo speed** command or the **speed auto** command, the auto-negotiation speed setting of the port restores to the default setting.
- The effect of executing **speed auto 10 100 1000** equals to that of executing **speed auto**, that is, the port is configured to support all the auto-negotiation speeds: 10 Mbps, 100 Mbps, and 1000 Mbps.

Setting the Ethernet Port Broadcast Suppression Ratio

You can use the **broadcast-suppression** commands to restrict the broadcast traffic allowed to pass through a port. After that, if the broadcast traffic on the port exceeds the value you set, the system will maintain an appropriate broadcast traffic ratio by discarding the overflow traffic, so as to suppress broadcast storm, avoid network congestion and ensure normal network services.

You can execute the **broadcast-suppression** command in system view or Ethernet port view:

- If you execute the command in system view, the command takes effect on all ports.
- If you execute the command in Ethernet port view, the command takes effect only on current port.

Follow these steps to set the Ethernet port broadcast suppression ratio:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the global broadcast suppression ratio	**broadcast-suppression** { *ratio* | **pps** *max-pps* }	By default, the ratio is 100%, that is, the system does not suppress broadcast traffic globally.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the broadcast suppression ratio on current port	**broadcast-suppression** { *ratio* | **pps** *max-pps* }	By default, the ratio is 100%, that is, the system does not suppress broadcast traffic on the port.

Enabling Flow Control on a Port

After flow control is enabled on both the local and the peer devices, if congestion occurs on the local device, the device will inform its peer to suspend packet sending or lower the packet sending rate. In this way, packet loss is reduced and normal network services are guaranteed.

Follow these steps to enable flow control on a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable flow control on the Ethernet port	**flow-control**	Required By default, flow control is not enabled on a port.

Configuring Access Port Attribute

Follow these steps to configure access port attribute:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the link type for the port as access	**port link-type access**	By default, the link type for the port is access.
Add the current access port into the specified VLAN	**port access vlan** *vlan-id*	Optional

Configuring Hybrid Port Attribute

Follow these steps to configure hybrid port attribute:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the link type for the port as hybrid	**port link-type hybrid**	Required
Set the default VLAN ID for the hybrid port	**port hybrid pvid vlan** *vlan-id*	Optional By default, the VLAN of a hybrid port is VLAN 1.
Add the current hybrid port into the specified VLAN	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Optional For a hybrid port, you can configure to tag the packets of specific VLANs, based on which the packets of those VLANs can be processed in differently ways.

Configuring Trunk Port Attribute

Follow these steps to configure trunk port attribute:

To do…	Use the command…	Remarks
Enter system view	**System-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the link type for the port as trunk	**port link-type trunk**	Required
Set the default VLAN ID for the trunk port	**port trunk pvid vlan** *vlan-id*	Optional By default, the VLAN of a trunk port is VLAN 1.
Add the current trunk port into the specified VLAN	**port trunk permit vlan** { *vlan-id-list* | **all** }	Optional

Disabling Up/Down Log Output on a Port

An Ethernet port has two physical link statuses: UP and Down. When the link status of an Ethernet port changes, the device sends log information to the log server, which then acts accordingly. If the status of Ethernet ports changes frequently, the device sends log information to the log server frequently, burdening the log server and consuming plenty of network resources.

To solve this problem, you can disable the Up/Down log output function on some ports, so as to reduce the quantity of log information output to the log server.

Note

After you allow a port to output the Up/Down log information, if the physical link status of the port does not change, the device does not send log information to the log server but monitors the port in real time.

Configuration tasks

Follow these steps to disable a port from outputting UP/Down log information:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Disable a port from outputting UP/Down Log Information	**undo enable log updown**	Required By default, a port is allowed to output the UP/Down log information.

Configuration example

By default, port GigabitEthernet 1/0/1 is allowed to output the Up/Down log information. Execute the **shutdown** command or the **undo shutdown** command on GigabitEthernet 1/0/1, and the system outputs Up/Down log information of GigabitEthernet 1/0/1.

```
<device> system-view
[device] interface GigabitEthernet 1/0/1
[device-GigabitEthernet1/0/1] shutdown
[device-GigabitEthernet1/0/1]
%Apr  2 08:11:14:220 2000 device L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 GigabitEthernet1/0/1 is DOWN
[device-GigabitEthernet1/0/1] undo shutdown
[device-GigabitEthernet1/0/1]
%Apr  2 08:11:32:253 2000 device L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 GigabitEthernet1/0/1 is UP
```

Disable GigabitEthernet 1/0/1 from outputting Up/Down log information, execute the **shutdown** command or the **undo shutdown** command on GigabitEthernet 1/0/1, and no Up/Down log information is output for GigabitEthernet 1/0/1.

```
[device-GigabitEthernet1/0/1] undo enable log updown
[device-GigabitEthernet1/0/1] shutdown
[device-GigabitEthernet1/0/1] undo shutdown
```

Copying Port Configuration to Other Ports

To make some other ports have the same configuration as that of a specific port, you can copy the configuration of the specific port to the ports.

Specifically, the following types of port configuration can be copied from one port to other ports: VLAN configuration, protocol-based VLAN configuration, LACP configuration, QoS configuration, GARP configuration, STP configuration and initial port configuration. For the detailed copy content, please refer to the Command Manual.

Follow these steps to copy port configuration to other ports:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Copy port configuration to other ports	**copy configuration source** { *interface-type interface-number* | **aggregation-group** *source-agg-id* } **destination** { *interface-list* [**aggregation-group** *destination-agg-id*] | **aggregation-group** *destination-agg-id* }	Required

Note

- If you specify the source aggregation group ID, the system uses the port with the smallest port number in the aggregation group as the source.
- If you specify the destination aggregation ID, the configuration of the source port will be copied to all ports in the aggregation group.

Configuring a Port Group

To make the configuration task easier for users, certain devices allow users to configure on a single port as well as on multiple ports in a port group. In port group view, the user only needs to input the

configuration command once on one port and that configuration will apply to all ports in the port group. This effectively reduces redundant configurations.

A Port group could be manually created by users. Multiple Ethernet ports can be added to the same port group but one Ethernet port can only be added to one port group.

Follow these steps to configure a port group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a port group or enter the specified port group view	**port-group** *group-id*	Required
Add an Ethernet port to a specified port group	**port** *interface-list*	Required



Note

A port can not be added to a port group if it has been added to an aggregation group, and vice versa.

Setting Loopback Detection for an Ethernet Port

Loopback detection is used to monitor if loopback occurs on a port.

After you enable loopback detection on Ethernet ports, the device can monitor if external loopback occurs on them. If there is a loopback port found, the device will put it under control.

- If loopback is found on an access port, the system disables the port, sends a Trap message to the client and removes the corresponding MAC forwarding entry.
- If loopback is found on a trunk or hybrid port, the system sends a Trap message to the client. When the loopback port control function is enabled on these ports, the system disables the port, sends a Trap message to the client and removes the corresponding MAC forwarding entry.

Follow these steps to set loopback detection for an Ethernet port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable loopback detection globally	**loopback-detection enable**	Required By default, loopback detection is disabled globally.
Set time interval for port loopback detection	**loopback-detection interval-time** *time*	Optional The default interval is 30 seconds.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable loopback detection on a specified port	**loopback-detection enable**	Required By default, port loopback detection is disabled.
Enable loopback port control on the trunk or hybrid port	**loopback-detection control enable**	Optional By default, loopback port control is not enabled.

To do…	Use the command…	Remarks
Configure the system to run loopback detection on all VLANs for the trunk and hybrid ports	**loopback-detection per-vlan enable**	Optional By default, the system runs loopback detection only on the default VLAN for the trunk and hybrid ports.

Caution

- To enable loopback detection on a specific port, you must use the **loopback-detection enable** command in both system view and the specific port view.
- After you use the **undo loopback-detection enable** command in system view, loopback detection will be disabled on all ports.
- The commands of loopback detection feature cannot be configured with the commands of port link aggregation at the same time.

Configuring the Ethernet Port to Run Loopback Test

You can configure the Ethernet port to run loopback test to check if it operates normally. The port running loopback test cannot forward data packets normally. The loopback test terminates automatically after a specific period.

Follow these steps to configure an Ethernet port to run loopback test:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the Ethernet port to run loopback test	**loopback** { **external** | **internal** }	Required

Note

- **external:** Performs external loop test. In the external loop test, self-loop headers (which are made from four cores of the 8-core cables) must be used on the ports of the device. The external loop test can locate the hardware failures on the port.
- **internal**: Performs internal loop test. In the internal loop test, self loop is established in the switching chip to locate the chip failure which is related to the port.

After you use the **shutdown** command on a port, the port cannot run loopback test. You cannot use the **speed**, **duplex**, **mdi** and **shutdown** commands on the ports running loopback test. Some ports do not support loopback test, and corresponding prompts will be given when you perform loopback test on them.

Enabling the System to Test Connected Cable

You can enable the system to test the cable connected to a specific port. The test result will be returned in five minutes. The system can test these attributes of the cable: Receive and transmit directions (RX and TX), short circuit/open circuit or not, the length of the faulty cable.

Follow these steps to enable the system to test connected cables:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the system to test connected cables	**virtual-cable-test**	Required

Note

- Optical port (including Combo optical port) does not support VCT (**virtual-cable-test**) function.
- Combo electrical port supports VCT function only when it is in UP condition (using undo shutdown command), normal Ethernet electrical port always supports this function.

Configuring the Interval to Perform Statistical Analysis on Port Traffic

By performing the following configuration, you can set the interval to perform statistical analysis on the traffic of a port.

When you use the **display interface** *interface-type interface-number* command to display the information of a port, the system performs statistical analysis on the traffic flow passing through the port during the specified interval and displays the average rates in the interval. For example, if you set this interval to 100 seconds, the displayed information is as follows:

Last 100 seconds input: 0 packets/sec 0 bytes/sec

Last 100 seconds output: 0 packets/sec 0 bytes/sec

Follow these steps to set the interval to perform statistical analysis on port traffic:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the interval to perform statistical analysis on port traffic	**flow-interval** *interval*	Optional By default, this interval is 300 seconds.

Displaying and Maintaining Ethernet Ports

To do…	Use the command…	Remarks
Display port configuration information	**display interface** [*interface-type* | *interface-type interface-number*]	Available in any view
Display information for a specified port group	**display port-group** *group-id*	
Display port loopback detection state	**display loopback-detection**	
Display brief configuration information about one or all ports	**display brief interface** [*interface-type* [*interface-number*]] [**|** { **begin** | **include** | **exclude** } *regular-expression*]	
Display current type-specific ports	**display port** { **hybrid** | **trunk** | **combo** }	
Display port information about a specified unit	**display unit** *unit-id* **interface**	
Clear the statistics of the port	**reset counters interface** [*interface-type* | *interface-type interface-number*]	After 802.1X is enabled, the port information cannot be reset.

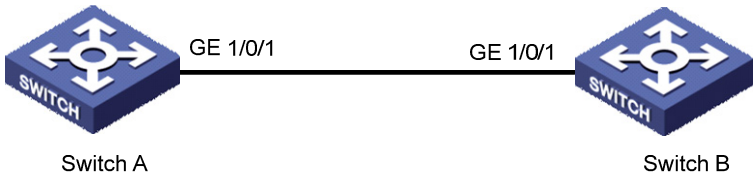
Ethernet Port Configuration Example

Network requirements

As shown in Figure 1-1:

- Switch A is connected to Switch B through trunk port GigabitEthernet 1/0/1.
- Configure the default VLAN ID for the trunk port as 100.
- Allow the packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass the port.

Figure 1-1 Network diagram for default VLAN ID configuration



Configuration procedure

The following configuration is used for Switch A. Configure Switch B in a similar way.

Enter port view of GigabitEthernet 1/0/1.

```
[device] interface GigabitEthernet1/0/1
```

Set GigabitEthernet 1/0/1 as a trunk port and allow the packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass the port.

```
[device-GigabitEthernet1/0/1] port link-type trunk
[device-GigabitEthernet1/0/1] port trunk permit vlan 2 6 to 50 100
```

Create VLAN 100.

```
[device] vlan 100
```

Configure the default VLAN ID of GigabitEthernet 1/0/1 as 100.

```
[device-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

Troubleshooting Ethernet Port Configuration

Symptom: Default VLAN ID configuration failed.

Solution: Take the following steps.

- Use the **display interface** or **display port** command to check if the port is a trunk port or a hybrid port. If not, configure it as a trunk port or a hybrid port.
- Configure the default VLAN ID.

Table of Contents

1 Link Aggregation Configuration ····· 1-1
Overview ····· 1-1
Introduction to Link Aggregation ····· 1-1
Introduction to LACP ····· 1-1
Operation Key ····· 1-2
Manual Aggregation Group ····· 1-2
Static LACP Aggregation Group ····· 1-3
Dynamic LACP Aggregation Group ····· 1-4
Aggregation Group Categories ····· 1-5
Link Aggregation Configuration ····· 1-6
Configuring a Manual Aggregation Group ····· 1-6
Configuring a Static LACP Aggregation Group ····· 1-7
Configuring a Dynamic LACP Aggregation Group ····· 1-8
Displaying and Maintaining Link Aggregation ····· 1-9
Link Aggregation Configuration Example ····· 1-9

1 Link Aggregation Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Overview

Introduction to Link Aggregation

Link aggregation means aggregating several ports together to form an aggregation group, so as to implement outgoing/incoming load sharing among the member ports in the group and to enhance the connection reliability.

Depending on different aggregation modes, link aggregation falls into three types: manual, static LACP, and dynamic LACP aggregations. Depending on whether or not load sharing is implemented, aggregation groups can be load-sharing or non-load-sharing aggregation groups.

For the member ports in an aggregation group, their basic configuration must be the same. The basic configuration includes STP, QoS, VLAN, port attributes and other associated settings.

- STP configuration, including STP status (enabled or disabled), link attribute (point-to-point or not), STP priority, path cost, standard packet format, maximum packet transmission speed, loop prevention status, root protection status, edge port or not.
- QoS configuration, including traffic limit, priority remarking, default 802.1p priority, bandwidth assurance, congestion avoidance, traffic redirection, traffic statistics, and so on.
- VLAN configuration, including permitted VLANs, and default VLAN ID.
- Port attribute configuration, including port rate, duplex mode, and link type (trunk, hybrid, or access).

Introduction to LACP

The purpose of link aggregation control protocol (LACP) is to implement dynamic link aggregation and deaggregation. This protocol is based on IEEE802.3ad and uses LACPDUs (link aggregation control protocol data unit) to interact with its peer.

After LACP is enabled on a port, LACP notifies the following information of the port to its peer by sending LACPDUs: priority and MAC address of this system, priority, number and operation key of the port. Upon receiving the information, the peer compares the information with the information of other ports on the peer device to determine the ports that can be aggregated. In this way, the two parties can reach an agreement in adding/removing the port to/from a dynamic aggregation group.

Operation Key

An operation key of an aggregation port is a configuration combination generated by system depending on the configurations of the port (rate, duplex mode, other basic configuration, and management key) when the port is aggregated.

1) The selected ports in a manual/static aggregation group have the same operation key.
2) The management key of an LACP-enabled static aggregation port is equal to its aggregation group ID.
3) The management key of an LACP-enabled dynamic aggregation port is zero by default.
4) The member ports in a dynamic aggregation group must have the same operation key.

Manual Aggregation Group

Introduction to manual aggregation group

A manual aggregation group is manually created. All its member ports are manually added and can be manually removed (it inhibits the system from automatically adding/removing ports to/from it). Each manual aggregation group must contain at least one port. When a manual aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

LACP is disabled on the member ports of manual aggregation groups, and enabling LACP on such a port will not take effect.

Port status in manual aggregation group

The selected port with the smallest port number serves as the master port of the group, and other selected ports serve as member ports of the group.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the member ports serving as selected ports in an aggregation group exceeds the maximum number supported by the device, the system will choose the ports with lower port numbers as the selected ports, and set others as unselected ports.

In a manual aggregation group, the system sets the ports to selected or unselected state by the following rules:

- Among the ports in an aggregation group that are in up state, the system determines the mater port with one of the following settings being the highest (in descending order) as the master port: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed. The ports with their rate, duplex mode and link type being the same as that of the master port are selected ports, and the rest are unselected ports.
- The system sets the ports unable to aggregate with the master port (due to some hardware limit) to unselected state.

Requirements on ports for manual aggregation

Generally, there is no limit on the rate and duplex mode of the ports (also including initially DOWN port) you want to add to a manual aggregation group. After aggregation, the smallest-numbered selected port is the master port of the aggregation group and the other selected ports are the member ports of the aggregation group.

Note

For an aggregation group:

- When the rate or duplex mode of a port in the aggregation group changes, packet loss may occur on this port;
- When the rate of a port decreases, if the port belongs to a manual or static LACP aggregation group, the port will be switched to the unselected state; if the port belongs to a dynamic LACP aggregation group, deaggregation will occur on the port.

Static LACP Aggregation Group

Introduction to static LACP aggregation

A static LACP aggregation group is also manually created. All its member ports are manually added and can be manually removed (it inhibits the system from automatically adding/removing ports to/from it). Each static aggregation group must contain at least one port. When a static aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

LACP is enabled on the member ports of static aggregation groups. When you remove a static aggregation group, all the member ports in up state form one or multiple dynamic aggregations with LACP enabled. LACP cannot be disabled on static aggregation ports.

Port status of static aggregation group

A port in a static aggregation group can be in one of the two states: selected or unselected.

- Both the selected and the unselected ports can transceive LACP protocol packets.
- Only the selected ports can transceive service packets; the unselected ports cannot.

In a static aggregation group, the system sets the ports to selected or unselected state according to the following rules.

- The system determines the master port with one of the following settings being the highest (in descending order) as the master port: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed. The ports with their rate, duplex mode and link type being the same as that of the master port are selected port.
- The ports connected to a peer device different from the one the master port is connected to or those connected to the same peer device as the master port but to a peer port that is not in the same aggregation group as the peer port of the master port are unselected ports.
- The ports unable to aggregate with the master port (due to some hardware limit) are unselected ports.
- The system sets the ports with basic port configuration different from that of the master port to unselected state.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the selected ports in an aggregation group exceeds the maximum number supported by the device, those with lower port numbers operate as the selected ports, and others as unselected ports.

Dynamic LACP Aggregation Group

Introduction to dynamic LACP aggregation group

A dynamic LACP aggregation group is automatically created and removed by the system. Users cannot add/remove ports to/from it. A port can participate in dynamic link aggregation only when it is LACP-enabled. Ports can be aggregated into a dynamic aggregation group only when they are connected to the same peer device and have the same basic configuration (such as rate and duplex mode).

Besides multiple-port aggregation groups, the system is also able to create single-port aggregation groups, each of which contains only one port. LACP is enabled on the member ports of dynamic aggregation groups.

Port status of dynamic aggregation group

A port in a dynamic aggregation group can be in one of the two states: selected or unselected. In a dynamic aggregation group, both the selected and the unselected ports can transceive LACP protocol packets; the selected ports can transceive user service packets, but the unselected ports cannot.



Note

In an aggregation group, the selected port with the smallest port number serves as the master port of the group, and other selected ports serve as member ports of the group.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the member ports that can be set as selected ports in an aggregation group exceeds the maximum number supported by the device, the system will negotiate with its peer end, to determine the states of the member ports according to the port IDs of the preferred device (that is, the device with smaller system ID). The following is the negotiation procedure:

1) Compare device IDs (system priority + system MAC address) between the two parties. First compare the two system priorities, then the two system MAC addresses if the system priorities are equal. The device with smaller device ID will be considered as the preferred one.
2) Compare port IDs (port priority + port number) on the preferred device. The comparison between two port IDs is as follows: First compare the two port priorities, then the two port numbers if the two port priorities are equal; the port with the smallest port ID is the selected port and the left ports are unselected ports.

Configuring system priority

LACP determines the selected and unselected states of the dynamic aggregation group members according to the priority of the port ID on the end with the preferred device ID.

The device ID consists of two-byte system priority and six-byte system MAC address, that is, device ID = system priority + system MAC address.

When two device IDs are compared, the system priorities are compared first, and the system MAC addresses are compared when the system priorities are the same. The device with smaller device ID will be considered as the preferred one.

Note

Changing the system priority of a device may change the preferred device between the two parties, and may further change the states (selected or unselected) of the member ports of dynamic aggregation groups.

Configuring port priority

LACP determines the selected and unselected states of the dynamic aggregation group members according to the port IDs on the device with the preferred device ID. When the number of members in an aggregation group exceeds the number of selected ports supported by the device in each group, LACP determines the selected and unselected states of the ports according to the port IDs. The ports with superior port IDs will be set to selected state and the ports with inferior port IDs will be set to unselected state.

The port ID consists of two-byte port priority and two-byte port number, that is, port ID = port priority + port number. When two port IDs are compared, the port priorities are compared first, and the port numbers are compared if the port priorities are the same.

Aggregation Group Categories

Depending on whether or not load sharing is implemented, aggregation groups can be load-sharing or non-load-sharing aggregation groups. When load sharing is implemented,

- For IP packets, the system will implement load-sharing based on source IP address and destination IP address;
- For non-IP packets, the system will implement load-sharing based on source MAC address and destination MAC address.

In general, the system only provides limited load-sharing aggregation resources, so the system needs to reasonably allocate the resources among different aggregation groups.

The system always allocates hardware aggregation resources to the aggregation groups with higher priorities. When load-sharing aggregation resources are used up by existing aggregation groups, newly-created aggregation groups will be non-load-sharing ones.

Load-sharing aggregation resources are allocated to aggregation groups in the following order:

- An aggregation group containing special ports (such as 10GE port) which require hardware aggregation resources has higher priority than any aggregation group containing no special port.
- A manual or static aggregation group has higher priority than a dynamic aggregation group (unless the latter contains special ports while the former does not).
- For aggregation groups, the one that might gain higher speed if resources were allocated to it has higher priority than others. If the groups can gain the same speed, the one with smallest master port number has higher priority than other groups.

When an aggregation group of higher priority appears, the aggregation groups of lower priorities release their hardware resources. For single-port aggregation groups, they can transceive packets normally without occupying aggregation resources

Caution

A load-sharing aggregation group contains at least two selected ports, but a non-load-sharing aggregation group can only have one selected port at most, while others are unselected ports.

Link Aggregation Configuration

Caution

- The commands of link aggregation cannot be configured with the commands of port loopback detection feature at the same time.
- The ports where the **mac-address max-mac-count** command is configured cannot be added to an aggregation group. Contrarily, the **mac-address max-mac-count** command cannot be configured on a port that has already been added to an aggregation group.
- MAC-authentication-enabled ports and 802.1x-enabled ports cannot be added to an aggregation group.
- Mirroring destination ports and mirroring reflector ports cannot be added to an aggregation group.
- Ports configured with blackhole MAC addresses, static MAC addresses or the static ARP protocol cannot be added to the aggregation group.
- Ports where the IP-MAC address binding is configured cannot be added to an aggregation group.
- Port-security-enabled ports cannot be added to an aggregation group.
- The port with Voice VLAN enabled cannot be added to an aggregation group.
- Do not add ports with IP filtering enabled to an aggregation group.
- Do not add ports with ARP intrusion detection enabled to an aggregation group.
- Do not add ports with source IP addresses/source MAC addresses statically bound to them to an aggregation group.
- A port belonging to a port group cannot be added to an aggregation group. Conversely, a port belonging to an aggregation group cannot be added to a port group.

Configuring a Manual Aggregation Group

You can create a manual aggregation group, or remove an existing manual aggregation group (after that, all the member ports in the group are removed from the ports).

For a manual aggregation group, a port can only be manually added/removed to/from the manual aggregation group.

Follow these steps to configure a manual aggregation group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a manual aggregation group	**link-aggregation group** *agg-id* **mode manual**	Required

To do…	Use the command…	Remarks
Configure a description for the aggregation group	**link-aggregation group** *agg-id* **description** *agg-name*	Optional By default, an aggregation group has no description.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add the Ethernet port to the aggregation group	**port link-aggregation group** *agg-id*	Required

Note that:

1) When creating an aggregation group:

- If the aggregation group you are creating already exists but contains no port, its type will change to the type you set.
- If the aggregation group you are creating already exists and contains ports, the possible type changes may be: changing from dynamic or static to manual, and changing from dynamic to static; and no other kinds of type change can occur.
- When you change a dynamic/static group to a manual group, the system will automatically disable LACP on the member ports. When you change a dynamic group to a static group, the system will remain the member ports LACP-enabled.

2) When a manual or static aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

Configuring a Static LACP Aggregation Group

You can create a static LACP aggregation group, or remove an existing static aggregation group (after that, the system will re-aggregate the original member ports in the group to form one or more dynamic aggregation groups.).

For a static aggregation group, a port can only be manually added/removed to/from the static aggregation group.

Note

When you add an LACP-enabled port to a manual aggregation group, the system will automatically disable LACP on the port. Similarly, when you add an LACP-disabled port to a static aggregation group, the system will automatically enable LACP on the port.

Follow these steps to configure a static LACP aggregation group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a static aggregation group	**link-aggregation group** *agg-id* **mode static**	Required

To do…	Use the command…	Remarks
Configure a description for the aggregation group	**link-aggregation group** *agg-id* **description** *agg-name*	Optional By default, an aggregation group has no description.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add the port to the aggregation group	**port link-aggregation group** *agg-id*	Required

Note

For a static LACP aggregation group or a manual aggregation group, you are recommended not to cross cables between the two devices at the two ends of the aggregation group. For example, suppose port 1 of the local device is connected to port 2 of the peer device. To avoid cross-connecting cables, do not connect port 2 of the local device to port 1 of the peer device. Otherwise, packets may be lost.

Configuring a Dynamic LACP Aggregation Group

A dynamic LACP aggregation group is automatically created by the system based on LACP-enabled ports. The adding and removing of ports to/from a dynamic aggregation group are automatically accomplished by LACP.

You need to enable LACP on the ports which you want to participate in dynamic aggregation of the system, because, only when LACP is enabled on those ports at both ends, can the two parties reach agreement in adding/removing ports to/from dynamic aggregation groups.

Note

You cannot enable LACP on a port which is already in a manual aggregation group.

Follow these steps to configure a dynamic LACP aggregation group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a description for an aggregation group	**link-aggregation group** *agg-id* **description** *agg-name*	Optional By default, an aggregation group has no description.
Configure the system priority	**lacp system-priority** *system-priority*	Optional By default, the system priority is 32,768.
Enter Ethernet port view	**interface** *interface-type interface-number*	—

To do…	Use the command…	Remarks
Enable LACP on the port	**lacp enable**	Required By default, LACP is disabled on a port.
Configure the port priority	**lacp port-priority** *port-priority*	Optional By default, the port priority is 32,768.

Displaying and Maintaining Link Aggregation

To do…	Use the command…	Remarks
Display summary information of all aggregation groups	**display link-aggregation summary**	You can execute the **display** command in any view.
Display detailed information of a specific aggregation group or all aggregation groups	**display link-aggregation verbose** [*agg-id*]	
Display link aggregation details of a specified port or port range	**display link-aggregation interface** *interface-type interface-number* [**to** *interface-type interface-number*]	
Display local device ID	**display lacp system-id**	
Clear LACP statistics about a specified port or port range	**reset lacp statistics** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]	Execute the **reset** command in user view.

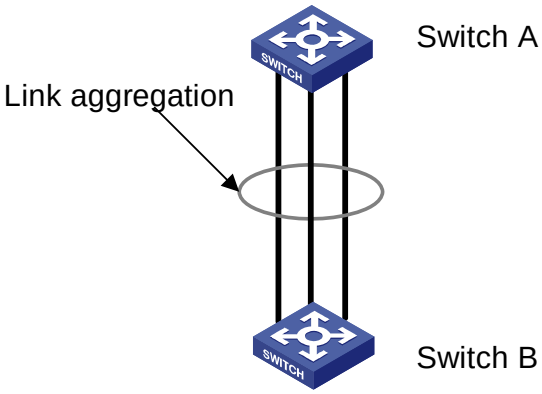
Link Aggregation Configuration Example

Network requirements

As shown in Figure 1-1:

- Switch A connects to Switch B with three ports GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3. It is required that incoming/outgoing load between the two switches can be shared among the three ports.
- Adopt three different aggregation modes to implement link aggregation on the three ports between switch A and B.

Figure 1-1 Network diagram for link aggregation configuration



Configuration procedure

1) Adopting manual aggregation mode

Create manual aggregation group 1.

```
<device> system-view
[device] link-aggregation group 1 mode manual
```

Add GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1.

```
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] port link-aggregation group 1
[device-GigabitEthernet1/0/1] interface GigabitEthernet1/0/2
[device-GigabitEthernet1/0/2] port link-aggregation group 1
[device-GigabitEthernet1/0/2] interface GigabitEthernet1/0/3
[device-GigabitEthernet1/0/3] port link-aggregation group 1
```

2) Adopting static LACP aggregation mode

Create static aggregation group 1.

```
<device> system-view
[device] link-aggregation group 1 mode static
```

Add GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1.

```
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] port link-aggregation group 1
[device-GigabitEthernet1/0/1] interface GigabitEthernet1/0/2
[device-GigabitEthernet1/0/2] port link-aggregation group 1
[device-GigabitEthernet1/0/2] interface GigabitEthernet1/0/3
[device-GigabitEthernet1/0/3] port link-aggregation group 1
```

3) Adopting dynamic LACP aggregation mode

Enable LACP on GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3.

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] lacp enable
[device-GigabitEthernet1/0/1] interface GigabitEthernet1/0/2
[device-GigabitEthernet1/0/2] lacp enable
[device-GigabitEthernet1/0/2] interface GigabitEthernet1/0/3
[device-GigabitEthernet1/0/3] lacp enable
```

Note that, the three LACP-enabled ports can be aggregated into a dynamic aggregation group to implement load sharing only when they have the same basic configuration (such as rate and duplex mode and so on).

Table of Contents

1 Port Isolation Configuration 1-1
Port Isolation Overview 1-1
Introduction to Port Isolation 1-1
Port Isolation Configuration 1-1
Displaying and Maintaining Port Isolation 1-2
Port Isolation Configuration Example 1-2

1 Port Isolation Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Port Isolation Overview

Introduction to Port Isolation

Through the port isolation feature, you can add the ports to be controlled into an isolation group to isolate the Layer 2 data between each port in the isolation group. Thus, you can improve the network security and network in a more flexible way.

Currently, you can configure only one isolation group on a switch. The number of Ethernet ports an isolation group can accommodate is not limited.

Note

The port isolation function is independent of VLAN configuration.

Port Isolation Configuration

Follow these steps to add an Ethernet port to an isolation group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-num*	—
Add the Ethernet port to the isolation group	**port isolate**	Required By default, an isolation group contains no port.

Note

- When a member port of an aggregation group is added to an isolation group, the other ports in the same aggregation group are added to the isolation group automatically.
- When a member port of an aggregation group is deleted from an isolation group, the other ports in the same aggregation group are deleted from the isolation group automatically.

Displaying and Maintaining Port Isolation

To do…	Use the command…	Remarks
Display the information about the Ethernet ports added to the isolation group.	**display isolate port**	Available in any view

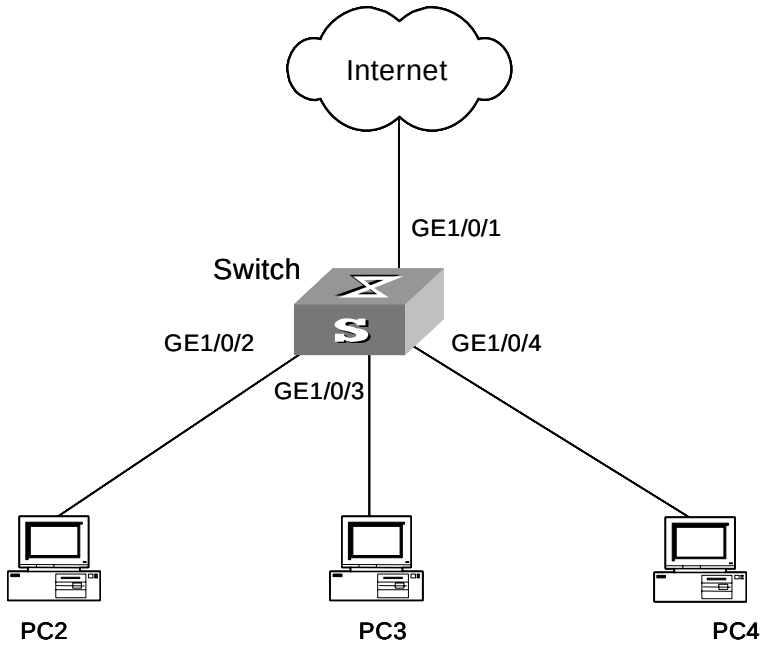
Port Isolation Configuration Example

Network requirements

As shown in Figure 1-1:

- PC 2, PC 3 and PC 4 are connected to GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4.
- The switch connects to the Internet through GigabitEthernet 1/0/1.
- It is desired that PC 2, PC 3 and PC 4 cannot communicate with each other.

Figure 1-1 Network diagram for port isolation configuration



Configuration procedure

Add GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to the isolation group.

```
<device> system-view
System View: return to User View with Ctrl+Z.
[device] interface GigabitEthernet1/0/2
[device-GigabitEthernet1/0/2] port isolate
[device-GigabitEthernet1/0/2] quit
[device] interface GigabitEthernet1/0/3
[device-GigabitEthernet1/0/3] port isolate
[device-GigabitEthernet1/0/3] quit
[device] interface GigabitEthernet1/0/4
[device-GigabitEthernet1/0/4] port isolate
[device-GigabitEthernet1/0/4] quit
[device]
```

Display the information about the ports in the isolation group.

```
[device] display isolate port
 Isolated port(s) on UNIT 1:
 GigabitEthernet1/0/2, GigabitEthernet1/0/3, GigabitEthernet1/0/4
```

Table of Contents

1 Port Security Configuration 1-1
Port Security Overview 1-1
Introduction 1-1
Port Security Features 1-1
Port Security Modes 1-2
Port Security Configuration 1-4
Enabling Port Security 1-4
Setting the Maximum Number of MAC Addresses Allowed on a Port 1-5
Setting the Port Security Mode 1-5
Configuring Port Security Features 1-6
Ignoring the Authorization Information from the RADIUS Server 1-8
Configuring Security MAC Addresses 1-8
Displaying and Maintaining Port Security Configuration 1-9
Port Security Configuration Example 1-9
2 Port Binding Configuration 2-1
Port Binding Overview 2-1
Introduction 2-1
Configuring Port Binding 2-1
Displaying and Maintaining Port Binding Configuration 2-1
Port Binding Configuration Example 2-2

1 Port Security Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Port Security Overview

Introduction

Port security is a security mechanism for network access control. It is an expansion to the current 802.1x and MAC address authentication.

Port security allows you to define various security modes that enable devices to learn legal source MAC addresses, so that you can implement different network security management as needed.

With port security enabled, packets whose source MAC addresses cannot be learned by the device in the security mode are considered illegal packets. The events that cannot pass 802.1x authentication or MAC authentication are considered illegal.

With port security enabled, upon detecting an illegal packet or illegal event, the system triggers the corresponding port security features and takes pre-defined actions automatically. This reduces your maintenance workload and greatly enhances system security and manageability.

Port Security Features

The following port security features are provided:

- NTK (need to know) feature: By checking the destination MAC addresses in outbound data frames on the port, NTK ensures that the device sends data frames through the port only to successfully authenticated devices, thus preventing illegal devices from intercepting network data.
- Intrusion protection feature: By checking the source MAC addresses in inbound data frames or the username and password in 802.1x authentication requests on the port, intrusion protection detects illegal packets or events and takes a pre-set action accordingly. The actions you can set include: disconnecting the port temporarily/permanently, and blocking packets with the MAC address specified as illegal.
- Trap feature: When special data packets (generated from illegal intrusion, abnormal login/logout or other special activities) are passing through a port on the device, device tracking enables the switch to send Trap messages to help the network administrator monitor special activities.

Port Security Modes

Table 1-1 describes the available port security modes.

Table 1-1 Description of port security modes

Security mode	Description	Feature
noRestriction	Port security is disabled on the port and access to the port is not restricted.	In this mode, neither the NTK nor the intrusion protection feature is triggered.
autolearn	In this mode, a port can learn a specified number of MAC addresses and save those addresses as secure MAC addresses. When the number of secure MAC addresses reaches the upper limit, the port changes to work in secure mode and permits only frames whose source MAC addresses are secure MAC addresses or static MAC addresses configured by using the mac-address static command.	In either mode, the device will trigger NTK and intrusion protection upon detecting an illegal packet.
secure	In this mode, the port is disabled from learning MAC addresses. Only those packets whose source MAC addresses are security MAC addresses learned and static or dynamic MAC addresses can pass through the port.	
userlogin	In this mode, port-based 802.1x authentication is performed for access users.	In this mode, neither NTK nor intrusion protection will be triggered.

Security mode	Description	Feature
userLoginSecure	In this mode, a port performs 802.1x authentication of users and services only one user passing 802.1x authentication at a time.	In any of these modes, the device triggers the NTK and Intrusion Protection features upon detecting an illegal packet or illegal event.
userLoginSecureExt	In this mode, a port performs 802.1x authentication of users and services users passing 802.1x authentication.	
userLoginWithOUI	Similar to the userLoginSecure mode, a port in this mode performs 802.1x authentication of users and services only one user passing 802.1x authentication. The differences include: Such a port also permits frames from a wired user whose MAC address contains a specified OUI (organizationally unique identifier). For frames from a wireless user, such a port performs OUI check at first. If the OUI check fails, the port performs 802.1x authentication.	
macAddressWithRadius	In this mode, a port performs RADIUS MAC authentication of users.	
macAddressOrUserLoginSecure	This mode is the combination of the userLoginSecure and macAddressWithRadius modes, with 802.1x authentication having a higher priority than MAC authentication. For a user using a wired connection, the port performs MAC authentication upon receiving non-802.1x frames and performs 802.1x authentication first upon receiving 802.1x frames. If 802.1x authentication fails, the port performs MAC authentication. For a wireless user, 802.1x authentication is performed first. If 802.1x authentication fails, MAC authentication is performed.	
macAddressOrUserLoginSecureExt	This mode is similar to the macAddressOrUserLoginSecure mode, except that there can be more than one 802.1x authenticated user on the port.	
macAddressElseUserLoginSecure	This mode is the combination of the macAddressWithRadius and userLoginSecure modes, with MAC authentication having a higher priority than 802.1x authentication. Upon receiving a non-802.1x frame, a port in this mode performs only MAC authentication. Upon receiving an 802.1x frame, the port performs MAC authentication and then, if MAC authentication fails, 802.1x authentication.	
macAddressElseUserLoginSecureExt	This mode is similar to the macAddressElseUserLoginSecure mode, except that there can be more than one 802.1x/MAC authenticated user on the port.	
macAddressAndUserLoginSecure	To perform 802.1x authentication on the access user, MAC authentication must be performed first. 802.1x authentication can be performed on the access user only if MAC authentication succeeds. In this mode there can be only one authenticated user on the port.	
macAddressAndUserLoginSecureExt	This mode is similar to the macAddressAndUserLoginSecure mode, except that there can be more than one authenticated user on the port.	

Port Security Configuration

Complete the following tasks to configure port security:

Task		Remarks
Enabling Port Security		Required
Setting the Maximum Number of MAC Addresses Allowed on a Port		Optional
Setting the Port Security Mode		Required
Configuring Port Security Features	Configuring the NTK feature	Optional Choose one or more features as required.
	Configuring intrusion protection	
	Configuring the Trap feature	
Ignoring the Authorization Information from the RADIUS Server		Optional
Configuring Security MAC Addresses		Optional

Enabling Port Security

Follow these steps to enable port security:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable port security	**port-security enable**	Required Disabled by default

Caution

Enabling port security resets the following configurations on the ports to the defaults (shown in parentheses below):

- 802.1x (disabled), port access control method (**macbased**), and port access control mode (**auto**)
- MAC authentication (disabled)

In addition, you cannot perform the above-mentioned configurations manually because these configurations change with the port security mode automatically.

Note

- For details about 802.1x configuration, refer to the sections covering 802.1x and System-Guard.
- For details about MAC authentication configuration, refer to the sections covering MAC authentication configuration.

Setting the Maximum Number of MAC Addresses Allowed on a Port

Port security allows more than one user to be authenticated on a port. The number of authenticated users allowed, however, cannot exceed the configured upper limit.

By setting the maximum number of MAC addresses allowed on a port, you can

- Control the maximum number of users who are allowed to access the network through the port
- Control the number of Security MAC addresses that can be added with port security

This configuration is different from that of the maximum number of MAC addresses that can be leaned by a port in MAC address management.

Follow these steps to set the maximum number of MAC addresses allowed on a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the maximum number of MAC addresses allowed on the port	**port-security max-mac-count** *count-value*	Required Not limited by default

Note

- Assume that, in the **macAddressOrUserLoginSecureExt** port security mode, you have configured to allow up to n authenticated users to access the network. When all of these n authenticated users are connected to the network and one or more of them are MAC-authenticated, to perform 802.1x authentication on the MAC-authenticated user(s), the number of maximum MAC addresses allowed on the port must be set to n + 1. Similarly, in the case of the **macAddressOrUserLoginSecure** security mode, the maximum number of MAC addresses allowed on the port must be set to 2.
- In the **macAddressAndUserLoginSecureExt** port security mode, to allow up to n authenticated users to be connected to the network at the same time and the nth user to be 802.1x-authenticated, the maximum number of MAC addresses allowed on the port must be set to at least n + 1. Similarly, in the case of the **macAddressAndUserLoginSecure** security mode, the maximum number of MAC addresses allowed on the port must be set to 2.

Setting the Port Security Mode

Follow these steps to set the port security mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the OUI value for user authentication	**port-security oui** *OUI-value* **index** *index-value*	Optional In **userLoginWithOUI** mode, a port supports one 802.1x user plus one user whose source MAC address has a specified OUI value.

To do…	Use the command…	Remarks
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the port security mode	**port-security port-mode** { **autolearn** | **mac-and-userlogin-secure** | **mac-and-userlogin-secure-ext** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }	Required By default, a port operates in **noRestriction** mode. In this mode, access to the port is not restricted. You can set a port security mode as needed.

Note

- Before setting the port security mode to **autolearn**, you need to set the maximum number of MAC addresses allowed on the port with the **port-security max-mac-count** command.
- After you set the port security mode to **autolearn**, you cannot configure any static or blackhole MAC addresses on the port.
- If the port is in a security mode other than **noRestriction**, before you can change the port security mode, you need to restore the port security mode to **noRestriction** with the **undo port-security port-mode** command.

If the **port-security port-mode** *mode* command has been executed on a port, none of the following can be configured on the same port:

- Maximum number of MAC addresses that the port can learn
- Reflector port for port mirroring
- Link aggregation

Configuring Port Security Features

Configuring the NTK feature

Follow these steps to configure the NTK feature:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the NTK feature	**port-security ntk-mode** { **ntkonly** | **ntk-withbroadcasts** | **ntk-withmulticasts** }	Required Be default, NTK is disabled on a port, namely all frames are allowed to be sent.

Note

The WX3000 series devices do not support the **ntkonly** NTK feature.

Configuring intrusion protection

Follow these steps to configure the intrusion protection feature:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the corresponding action to be taken by the device when intrusion protection is triggered	**port-security intrusion-mode** { **disableport** | **disableport-temporarily** | **blockmac** }	Required By default, no action is taken when intrusion protection is triggered.
Return to system view	**quit**	—
Set the timer during which the port remains disabled	**port-security timer disableport** *timer*	Optional 20 seconds by default

Note

The **port-security timer disableport** command is used in conjunction with the **port-security intrusion-mode disableport-temporarily** command to set the length of time during which the port remains disabled.

Caution

If you configure the NTK feature and execute the **port-security intrusion-mode blockmac** command on the same port, the device will be unable to disable the packets whose destination MAC address is illegal from being sent out that port; that is, the NTK feature configured will not take effect on the packets whose destination MAC address is illegal.

Configuring the Trap feature

Follow these steps to configure port security trapping:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable sending traps for the specified type of event	**port-security trap** { **addresslearned** | **intrusion** | **dot1xlogon** | **dot1xlogoff** | **dot1xlogfailure** | **ralmlogon** | **ralmlogoff** | **ralmlogfailure** }	Required By default, no trap is sent.

Ignoring the Authorization Information from the RADIUS Server

After an 802.1x user or MAC-authenticated user passes Remote Authentication Dial-In User Service (RADIUS) authentication, the RADIUS server delivers the authorization information to the device. You can configure a port to ignore the authorization information from the RADIUS server.

Follow these steps to configure a port to ignore the authorization information from the RADIUS server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Ignore the authorization information from the RADIUS server	**port-security authorization ignore**	Required By default, a port uses the authorization information from the RADIUS server.

Configuring Security MAC Addresses

Security MAC addresses are special MAC addresses that never age out. One security MAC address can be added to only one port in the same VLAN so that you can bind a MAC address to one port in the same VLAN.

Security MAC addresses can be learned by the auto-learn function of port security or manually configured.

Before adding security MAC addresses to a port, you must configure the port security mode to **autolearn**. After this configuration, the port changes its way of learning MAC addresses as follows.

- The port deletes original dynamic MAC addresses;
- If the amount of security MAC addresses has not yet reach the maximum number, the port will learn new MAC addresses and turn them to security MAC addresses;
- If the amount of security MAC addresses reaches the maximum number, the port will not be able to learn new MAC addresses and the port mode will be changed from **autolearn** to **secure**.

Note

The security MAC addresses manually configured are written to the configuration file; they will not get lost when the port is up or down. As long as the configuration file is saved, the security MAC addresses can be restored after the device reboots.

Configuration prerequisites

- Port security is enabled.
- The maximum number of security MAC addresses allowed on the port is set.
- The security mode of the port is set to **autolearn**.

Configuration procedure

Follow these steps to configure a security MAC address

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Add a security MAC address	In system view	**mac-address security** *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	Either is required. By default, no security MAC address is configured.
	In Ethernet port view	**interface** *interface-type interface-number*	
		mac-address security *mac-address* **vlan** *vlan-id*	

Displaying and Maintaining Port Security Configuration

To do…	Use the command…	Remarks
Display information about port security configuration	**display port-security** [**interface** *interface-list*]	Available in any view
Display information about security MAC address configuration	**display mac-address security** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]	

Port Security Configuration Example

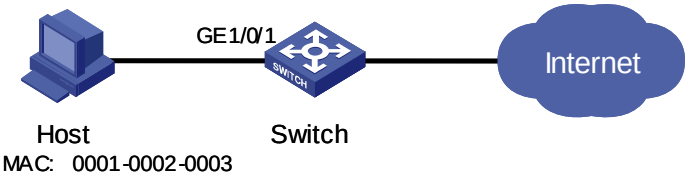
Network requirements

As shown in Figure 1-1, implement access user restrictions through the following configuration on GigabitEthernet 1/0/1 of the switch.

- Allow a maximum of 80 users to access the port without authentication and permit the port to learn and add the MAC addresses of the users as security MAC addresses.

- To ensure that Host can access the network, add the MAC address 0001-0002-0003 of Host as a security MAC address to the port in VLAN 1.
- After the number of security MAC addresses reaches 80, the port stops learning MAC addresses. If any frame with an unknown MAC address arrives, intrusion protection is triggered and the port will be disabled and stay silent for 30 seconds.

Figure 1-1 Network diagram for port security configuration



Configuration procedure

Enter system view.

```
<device> system-view
```

Enable port security.

```
[device] port-security enable
```

Enter GigabitEthernet 1/0/1 port view.

```
[device] interface GigabitEthernet 1/0/1
```

Set the maximum number of MAC addresses allowed on the port to 80.

```
[device-GigabitEthernet1/0/1] port-security max-mac-count 80
```

Set the port security mode to **autolearn**.

```
[device-GigabitEthernet1/0/1] port-security port-mode autolearn
```

Add the MAC address 0001-0002-0003 of Host as a security MAC address to the port in VLAN 1.

```
[device-GigabitEthernet1/0/1] mac-address security 0001-0002-0003 vlan 1
```

Configure the port to be silent for 30 seconds after intrusion protection is triggered.

```
[device-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[device-GigabitEthernet1/0/1] quit
[device] port-security timer disableport 30
```

2 Port Binding Configuration

Port Binding Overview

Introduction

Port binding enables the network administrator to bind the MAC address and IP address of a user to a specific port. After the binding, the switch forwards only the packets received on the port whose MAC address and IP address are identical with the bound MAC address and IP address. This improves network security and enhances security monitoring.

Configuring Port Binding

Follow these steps to configure port binding:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Bind the MAC address and IP address of a user to a specific port	In system view	**am user-bind mac-addr** *mac-address* **ip-addr** *ip-address* **interface** *interface-type interface-number*	User either approach. By default, no user MAC address or IP address is bound to a port.
	In Ethernet port view	**interface** *interface-type interface-number*	
		am user-bind mac-addr *mac-address* **ip-addr** *ip-address*	

Note

- An IP address can be bound to only one port at a time.
- A MAC address can be bound to only one port at a time.

Displaying and Maintaining Port Binding Configuration

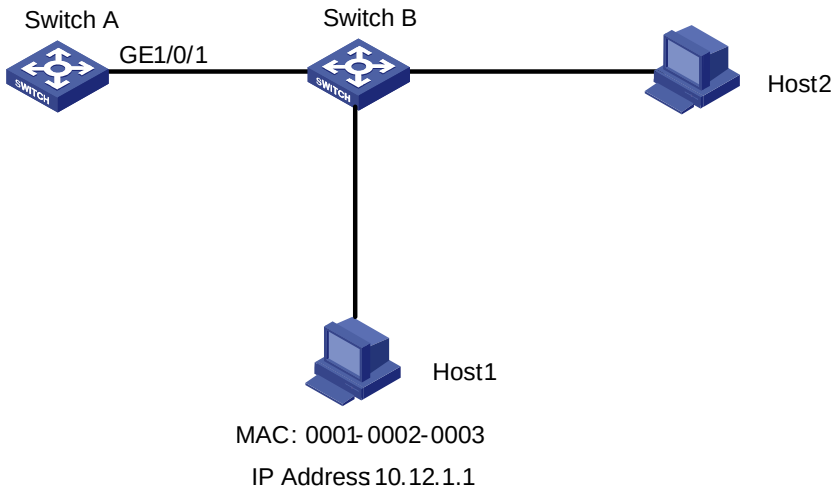
To do…	Use the command…	Remarks
Display port binding information	**display am user-bind** [**interface** *interface-type interface-number* | **ip-addr** *ip-addr* | **mac-addr** *mac-addr*]	Available in any view

Port Binding Configuration Example

Network requirements

As shown in Figure 2-1, it is required to bind the MAC and IP addresses of Host 1 to GigabitEthernet 1/0/1 on switch A, so as to prevent malicious users from using the IP address they steal from Host 1 to access the network.

Figure 2-1 Network diagram for port binding configuration



Configuration procedure

Configure switch A as follows:

Enter system view.

```
<device> system-view
```

Enter GigabitEthernet 1/0/1 port view.

```
[device] interface GigabitEthernet 1/0/1
```

Bind the MAC address and the IP address of Host 1 to GigabitEthernet 1/0/1.

```
[device-GigabitEthernet1/0/1] am user-bind mac-addr 0001-0002-0003 ip-addr 10.12.1.1
```

Table of Contents

1 DLDP Configuration 1-1
DLDP Overview 1-1
DLDP Fundamentals 1-2
Precautions During DLDP Configuration 1-6
DLDP Configuration 1-6
DLDP Configuration Tasks 1-6
Resetting DLDP Status 1-7
DLDP Network Example 1-8

1 DLDP Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

DLDP Overview

You may have encountered unidirectional links in networking, as shown in Figure 1-1 and Figure 1-2. When a unidirectional link occurs, the local device can receive packets from the peer device through the link layer, but the peer device cannot receive packets from the local device. Unidirectional links can cause many problems, such as spanning tree topology loop.

Device Link Detection Protocol (DLDP) can detect the link status of the optical fiber cable or copper twisted pair (such as super category 5 twisted pair). If DLDP finds a unidirectional link, it disables the related ports automatically or informs users to disable them manually according to the configurations, to avoid network problems.

Figure 1-1 Fiber cross-connection

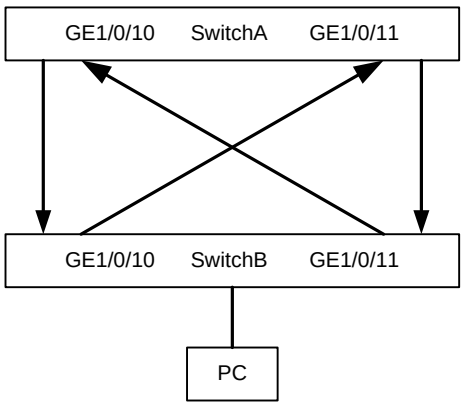
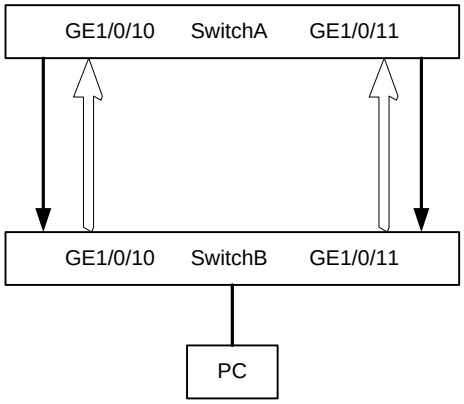


Figure 1-2 Fiber correct connection/disconnection in one direction



DLDP provides the following features:

- As a link layer protocol, it works together with the physical layer protocols to monitor the link status of a device. While the auto-negotiation mechanism on the physical layer detects physical signals and faults; DLDP identifies peer devices and unidirectional links, and disables unreachable ports.
- Even if the links of both ends can normally operate individually on the physical layer, DLDP can detect (at the link layer) whether these links are connected correctly and packets can be exchanged normally between the two ends. This detection cannot be implemented by the auto-negotiation mechanism.

Note

- When the port works in mandatory full duplex mode and the mandatory rate, DLDP can detect fiber disconnection in one direction as shown in Figure 1-2.
- When the port works in auto-negotiation duplex mode and auto-negotiation rate, even if DLDP is enabled, it does not take effect when fiber in one direction is disconnected as shown in Figure 1-2, in that case, it considers that the port is down.

DLDP Fundamentals

DLDP status

A link can be in one of these DLDP states: initial, inactive, active, advertisement, probe, disable, and delaydown.

Table 1-1 DLDP status

Status	Description
Initial	DLDP is not enabled.
Inactive	DLDP is enabled but the corresponding link is down
Active	DLDP is enabled and the link is up, or an neighbor entry is cleared
Advertisement	All neighbors communicate normally in both direction, or DLDP remains in active status for more than five seconds and enters this status. It is a stable status when no unidirectional link is found

Status	Description
Probe	DHCP sends packets to check if it is a unidirectional link. It enables the probe sending timer and an echo waiting timer for each target neighbor.
Disable	DLDP detects a unidirectional link, or finds (in enhanced mode) that a neighbor disappears. In this case, DLDP does not receive or send DLDP packets.
Delaydown	When a device in the active, advertisement, or probe DLDP state receives a port down message, it does not removes the corresponding neighbor immediately, neither does it changes to the inactive state. Instead, it changes to the delaydown state first. When a device changes to the delaydown state, the related DLDP neighbor information remains, and the Delaydown timer is triggered.

DLDP timers

DLDP works with the following timers:

Table 1-2 DLDP timers

Timer	Description
Advertisement sending timer	Interval of sending advertisement packets, which can be configured with a command line. By default, the interval is 5 seconds.
Probe sending timer	The interval is 0.5 second. In probe status, DLDP sends two probe packets every second.
Echo waiting timer	It is enabled when DLDP enters probe status. The timeout time is 10 seconds. If no echo packet is received from the neighbor when the Echo waiting timer expires, the local end is set to unidirectional communication status and the state machine turns into disable status. DLDP outputs log and tracking information, sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompt the user to disable the port manually. At the same time, DLDP deletes the neighbor entry.
Entry aging timer	When a new neighbor joins, a neighbor entry is created, and the corresponding entry aging timer is enabled. When an advertisement packet is received from a neighbor, the neighbor entry is updated, and the corresponding entry aging timer is updated. In normal mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP sends an advertisement packet with RSY tag, and deletes the neighbor entry. In enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer. The interval set for the entry aging timer is three times of that for the advertisement timer.

Timer	Description
Enhanced timer	In enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer for the neighbor. The timeout time for the enhanced timer is 10 seconds. The enhanced timer then sends one probe packets every one second and totally eight packets continuously to the neighbor. If no echo packet is received from the neighbor when the Enhanced timer expires, the local end is set to unidirectional communication status and the state machine turns into disable status. DLDP outputs log and tracking information, and sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompt the user to disable the port manually. DLDP deletes the neighbor entry.
Delaydown timer	When a device in the active, advertisement, or probe DLDP state receives a port down message, it does not removes the corresponding neighbor immediately, neither does it changes to the inactive state. Instead, it changes to the delaydown state first. When a device changes to the delaydown state, the related DLDP neighbor information remains, and the Delaydown timer is triggered. The Delaydown timer is configurable and ranges from 1 to 5 seconds. A device in the delaydown state only responds to port up messages. A device in the delaydown state resumes its original DLDP state if it receives a port up message before the delaydown timer expires. Otherwise, it removes the DLDP neighbor information and changes to the inactive state.

DLDP operating mode

DLDP can operate in two modes: normal and enhanced.

Table 1-3 DLDP operating mode and neighbor entry aging

DLDP operating mode	Whether DLDP probes neighbor during neighbor entry aging	Whether entry aging timer is enabled during neighbor entry aging	Whether enhanced timer is enabled when entry aging timer expire
Normal mode	No	Yes (the neighbor entry ages after the entry aging timer expires)	No
Enhanced mode	Yes	Yes (the enhanced timer is enabled after the entry aging timer expires)	Yes (When the enhanced timer expires, the local end is set to single pass status, and the neighbor entry ages)

DLDP implementation

1) If the DLDP-enabled link is up, DLDP sends DLDP packets to the peer device, and analyses and processes DLDP packets received from the peer device. DLDP in different status sends different packets.

Table 1-4 Types of packets sent by DLDP

DLDP status	Packet types
Active	Advertisement packets, including those with or without RSY tags
Advertisement	Advertisement packets
Probe	Probe packets

2) DLDP analyzes and processes received packets as follows:

- In authentication mode, DLDP authenticates the packets, and discards those do not pass the authentication.
- DLDP processes the received DLDP packets.

Table 1-5 Process received DLDP packets

<table>
<tr><th>Packet type</th><th colspan="5">Processing procedure</th></tr>
<tr><td rowspan="2">Advertisement packet</td><td colspan="2" rowspan="2">Extract neighbor information</td><td colspan="3">If this neighbor entry does not exist on the local device, DLDP creates the neighbor entry, enables the entry aging timer, and turns to probe status.</td></tr>
<tr><td colspan="3">If the neighbor entry already exists on the local device, DLDP refreshes the entry aging timer.</td></tr>
<tr><td>Flush packet</td><td colspan="5">Delete the neighbor entry from the local device</td></tr>
<tr><td rowspan="2">Probe packet</td><td colspan="2" rowspan="2">Send echo packets containing both neighbor and its own information to the peer</td><td colspan="3">Create the neighbor entry if this neighbor entry does not exist on the local device.</td></tr>
<tr><td colspan="3">If the neighbor entry already exists on the local device, refresh the entry aging timer.</td></tr>
<tr><td rowspan="4">Echo packet</td><td rowspan="4">Check whether the local device is in probe status</td><td>No</td><td colspan="3">Discard this echo packet</td></tr>
<tr><td rowspan="3">Yes</td><td rowspan="3">Check whether neighbor information in the packet is the same as that on the local device</td><td>No</td><td>Discard this echo packet</td></tr>
<tr><td rowspan="2">Yes</td><td>Set the neighbor flag bit to bidirectional</td></tr>
<tr><td>If all neighbors are in bidirectional communication state, DLDP turns from probe status to advertisement status, and sets the echo waiting timer to 0.</td></tr>
</table>

3) If no echo packet is received from the neighbor, DLDP performs the following processing:

Table 1-6 Processing when no echo packet is received from the neighbor

No Echo packet received from the neighbor	Processing procedure
In normal mode, no echo packet is received when the echo waiting timer expires	DLDP turns into disable status. It outputs log and tracking information, sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompt the user to disable the port manually. DLDP sends the RSY message and deletes the neighbor entry.
In enhanced mode, no echo packet is received when the enhanced timer expires	

DLDP neighbor state

A DLDP neighbor can be in one of these two states: two way and unknown. You can check the state of a DLDP neighbor by using the **display dldp** command.

Table 1-7 Description on the two DLDP neighbor states

DLDP neighbor state	Description
two way	The link to the neighbor operates properly.
unknown	The device is detecting the neighbor and the neighbor state is unknown.

Precautions During DLDP Configuration

- DLDP works only when the link is up.
- To insure unidirectional links can be detected, you must make sure: DLDP is enabled on both ends, and the interval of sending advertisement packets, authentication mode and password are consistent on both ends.
- You can adjust the interval of sending advertisement packets in different network circumstances, so that DLDP can respond rapidly to link failure. The interval must be shorter than one-third of the STP convergence time, which is generally 30 seconds. If too long an interval is set, an STP loop may occur before DLDP shut down unidirectional links. On the contrary, if too short an interval is set, network traffic increases, and port bandwidth is reduced.
- DLDP does not process any LACP event, and treats each link in the aggregation group as independent.

DLDP Configuration

DLDP Configuration Tasks

Follow these steps to configure DLDP:

<table>
<tr><th colspan="3">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="3">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td rowspan="3">Enable DLDP</td><td colspan="2">Enable DLDP globally</td><td>dldp enable</td><td rowspan="3">Required. By default, DLDP is disabled</td></tr>
<tr><td rowspan="2">Enable DLDP on a port</td><td>Enter Ethernet port view</td><td>Interface interface-type interface-number</td></tr>
<tr><td>Enable DLDP on a port</td><td>dldp enable</td></tr>
<tr><td colspan="3">Set the authentication mode and password</td><td>dldp authentication-mode { none | simple simple-password | md5 md5-password }</td><td>Optional. By default, the authentication mode is none</td></tr>
<tr><td colspan="3">Set the interval of sending DLDP packets</td><td>dldp interval integer</td><td>Optional. By default, the interval is 5 seconds.</td></tr>
</table>

To do…	Use the command…	Remarks
Set the delaydown timer	**dldp delaydown-timer** *delaydown-time*	Optional By default, the delaydown timer expires after 1 second it is triggered.
Set the DLDP handling mode when an unidirectional link is detected	**dldp unidirectional-shutdown** { **auto** | **manual** }	Optional. By default, the handling mode is auto.
Set the DLDP operating mode	**dldp work-mode** { **enhance** | **normal** }	Optional. By default, DLDP works in normal mode.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Display the configuration information about the DLDP-enabled ports	**display dldp** { *unit-id* | *interface-type interface-number* }	You can execute this command in any view.

Note

- When you use the **dldp enable/dldp disable** command in system view to enable/disable DLDP globally on all optical ports of the device, this command is only valid for existing optical ports on the device, however, it is not valid for those added subsequently.
- DLDP can operate normally only when the same authentication mode and password are set for local and peer ports.

Resetting DLDP Status

Note

The command here is only valid for those ports that are DLDP down due to the detection of unidirectional link. You can use the command here to reset the DLDP status of these ports to retrieve DLDP probes.

Follow these steps to reset DLDP status:

To do…	Use the command…	Remarks
Enter system view	**system-view**	Optional
Reset the DLDP status of the system	**dldp reset**	
Enter Ethernet port view	**interface** *interface-type interface-number*	
Reset the DLDP status of a port	**dldp reset**	

Caution

This command only applies to the ports in DLDP down status.

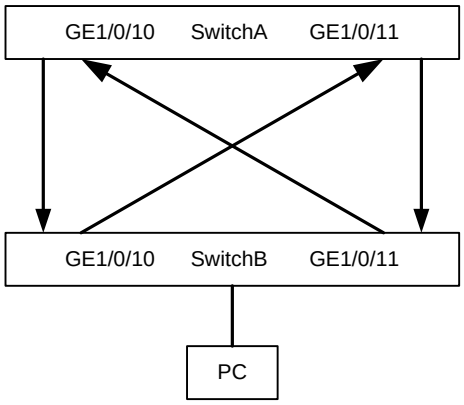
DLDP Network Example

Network requirements

As shown in Figure 1-3:

- Switch A and Switch B are connected through two pairs of fibers. Both of them support DLDP;
- Suppose the fibers between Switch A and Switch B are connected inversely. DLDP disconnects the unidirectional links after discovering them;
- When the network administrator connects the fiber correctly, the ports taken down by DLDP are restored.

Figure 1-3 Fiber cross-connection



Configuration procedure

1) Configure Switch A

Configure the ports to work in mandatory full duplex mode at the speed of 1000 Mbps.

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/10
[SwitchA-GigabitEthernet1/0/10] duplex full
[SwitchA-GigabitEthernet1/0/10] speed 1000
[SwitchA-GigabitEthernet1/0/10] quit
[SwitchA] interface gigabitethernet 1/0/11
```

```
[SwitchA-GigabitEthernet1/0/11] duplex full
[SwitchA-GigabitEthernet1/0/11] speed 1000
[SwitchA-GigabitEthernet1/0/11] quit
```

Enable DLDP globally

```
[SwitchA] dldp enable
 DLDP is enabled on all fiber ports except fabric ports.
```

Set the interval of sending DLDP packets to 15 seconds

```
[SwitchA] dldp interval 15
```

Configure DLDP to work in enhanced mode

```
[SwitchA] dldp work-mode enhance
```

Set the DLDP handling mode for unidirectional links to auto

```
[SwitchA] dldp unidirectional-shutdown auto
```

Display the DLDP status

```
[SwitchA] display dldp 1
```

 **Note**

When two switches are connected through fibers in a crossed way, two or three ports may be in the disable state, and the rest in the inactive state.

When a fiber is connected to a device correctly on one end with the other end connected to no device:

- If the device operates in the normal DLDP mode, the end that receives optical signals is in the advertisement state; the other end is in the inactive state.
- If the device operates in the enhance DLDP mode, the end that receives optical signals is in the disable state; the other end is in the inactive state.

Restore the ports taken down by DLDP

```
[SwitchA] dldp reset
```

2) Configure Switch B

The configuration of Switch B is the same to that of Switch A.

Table of Contents

1 MAC Address Table Management 1-1
Overview 1-1
Introduction to MAC Address Table 1-1
Introduction to MAC Address Learning 1-1
Managing MAC Address Table 1-3
Configuring MAC Address Table Management 1-4
Configuration Task List 1-4
Configuring a MAC Address Entry 1-5
Setting the Aging Time of MAC Address Entries 1-6
Setting the Maximum Number of MAC Addresses a Port Can Learn 1-6
Disabling MAC Address learning for a VLAN 1-7
Displaying and Maintaining MAC Address Table 1-8
Configuration Example 1-8
Adding a Static MAC Address Entry Manually 1-8

1 MAC Address Table Management

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.
- This chapter describes the management of static, dynamic, and blackhole MAC address entries. For information about the management of multicast MAC address entries, refer to the part related to multicast protocol.

Overview

Introduction to MAC Address Table

A switch is mainly used to forward packets at the data link layer, that is, transmit the packets to the corresponding ports according to the destination MAC address of the packets. To forward packets quickly, a switch maintains a MAC address table, which is a Layer 2 address table recording the MAC address-to-forwarding port association. Each entry in a MAC address table contains the following fields:

- Destination MAC address
- ID of the VLAN which a port belongs to
- Forwarding egress port numbers on the local switch

When forwarding a packet, a switch adopts one of the two forwarding methods based on the MAC address table entries.

- Unicast forwarding: If the destination MAC address carried in the packet is included in a MAC address table entry, the device forwards the packet through the forwarding egress port in the entry.
- Broadcast forwarding: If the destination MAC address carried in the packet is not included in the MAC address table, the device broadcasts the packet to all ports except the one receiving the packet.

Introduction to MAC Address Learning

MAC address table entries can be updated and maintained through the following two ways:

- Manual configuration
- MAC address learning

Generally, the majority of MAC address entries are created and maintained through MAC address learning. The following describes the MAC address learning process of the device:

1) As shown in Figure 1-1, User A and User B are both in VLAN 1. When User A communicates with User B, the packet from User A needs to be transmitted to GigabitEthernet 1/0/1. At this time, the device records the source MAC address of the packet, that is, the address “MAC-A” of User A to the MAC address table of the switch, forming an entry shown in Figure 1-2.

Figure 1-1 MAC address learning diagram (1)

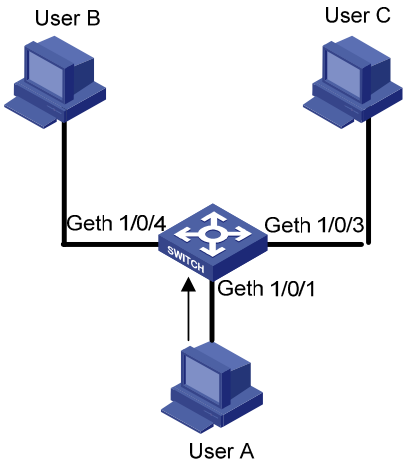
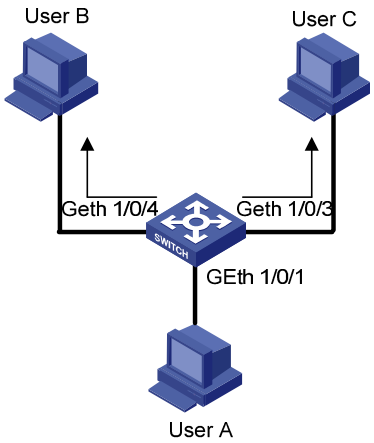


Figure 1-2 MAC address table entry of the switch (1)

MAC-address	Port	VLAN ID
MAC-A	GigabitEthernet1/0/1	1

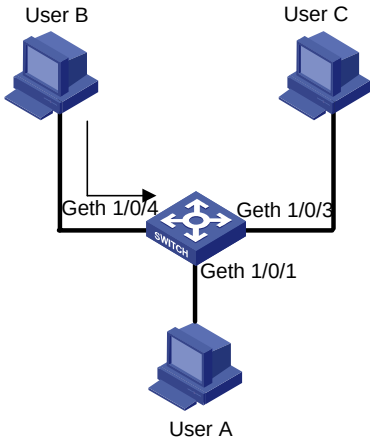
2) After learning the MAC address of User A, the device starts to forward the packet. Because there is no MAC address and port information of User B in the existing MAC address table, the device forwards the packet to all ports except GigabitEthernet 1/0/1 to ensure that User B can receive the packet.

Figure 1-3 MAC address learning diagram (2)



3) Because the device broadcasts the packet, both User B and User C can receive the packet. However, User C is not the destination device of the packet, and therefore does not process the packet. Normally, User B will respond to User A, as shown in Figure 1-4. When the response packet from User B is sent to GigabitEthernet 1/0/4, the device records the association between the MAC address of User B and the corresponding port to its MAC address table.

Figure 1-4 MAC address learning diagram (3)



4) At this time, the MAC address table of the device includes two forwarding entries shown in Figure 1-5. When forwarding the response packet, the device unicasts the packet instead of broadcasting it to User A through GigabitEthernet 1/0/1, because MAC-A is already in the MAC address table.

Figure 1-5 MAC address table entries of the switch (2)

MAC-address	Port	VLAN ID
MAC-A	GigabitEthernet1/0/1	1
MAC-B	GigabitEthernet1/0/4	1

5) After this interaction, the device directly unicasts the communication packets between User A and User B based on the corresponding MAC address table entries.

Note

- Under some special circumstances, for example, User B is unreachable or User B receives the packet but does not respond to it, the device cannot learn the MAC address of User B. Hence, the device still broadcasts the packets destined for User B.
- The device learns only unicast addresses by using the MAC address learning mechanism but directly drops any packet with a broadcast source MAC address.

Managing MAC Address Table

Aging of MAC address table

To fully utilize a MAC address table, which has a limited capacity, the device uses an aging mechanism for updating the table. That is, the device starts an aging timer for an entry when dynamically creating the entry, and removes the MAC address entry if no more packets with the MAC address recorded in the entry are received within the aging time.

Note

Aging timer only takes effect on dynamic MAC address entries.

Entries in a MAC address table

Entries in a MAC address table fall into the following categories according to their characteristics and configuration methods:

- Static MAC address entry: Also known as permanent MAC address entry. This type of MAC address entries are added/removed manually and can not age out by themselves. Using static MAC address entries can reduce broadcast packets remarkably and are suitable for networks where network devices seldom change.
- Dynamic MAC address entry: Dynamic MAC address entries age out after the configured aging time. They are generated by the MAC address learning mechanism or configured manually.
- Blackhole MAC address entry: Blackhole MAC address entries are configured manually. The device discards the packets destined for or originated from the MAC addresses contained in blackhole MAC address entries.

Table 1-1 lists the different types of MAC address entries and their characteristics.

Table 1-1 Characteristics of different types of MAC address entries

MAC address entry	Configuration method	Aging time	Reserved or not at reboot (if the configuration is saved)
Static MAC address entry	Manually configured	Unavailable	Yes
Dynamic MAC address entry	Manually configured or generated by MAC address learning mechanism	Available	No
Blackhole MAC address entry	Manually configured	Unavailable	Yes

Configuring MAC Address Table Management

Configuration Task List

Complete the following tasks to configure MAC address table management:

Task	Remarks
Configuring a MAC Address Entry	Required
Setting the Aging Time of MAC Address Entries	Optional
Setting the Maximum Number of MAC Addresses a Port Can Learn	Optional
Disabling MAC Address learning for a VLAN	Optional

Configuring a MAC Address Entry

You can add, modify, or remove a MAC address entry, remove all MAC address entries concerning a specific port, or remove specific type of MAC address entries (dynamic or static MAC address entries).

You can add a MAC address entry in either system view or Ethernet port view.

Adding a MAC address entry in system view

Follow these steps to add a MAC address entry in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Add a MAC address entry	**mac-address** { **static** | **dynamic** | **blackhole** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	Required

Caution

- When you add a MAC address entry, the port specified by the **interface** argument must belong to the VLAN specified by the **vlan** argument in the command. Otherwise, the entry will not be added.
- If the VLAN specified by the **vlan** argument is a dynamic VLAN, after a static MAC address is added, it will become a static VLAN.

Adding a MAC address entry in Ethernet port view

Follow these steps to add a MAC address entry in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add a MAC address entry	**mac-address** { **static** | **dynamic** | **blackhole** } *mac-address* **vlan** *vlan-id*	Required

Caution

- When you add a MAC address entry, the current port must belong to the VLAN specified by the **vlan** argument in the command. Otherwise, the entry will not be added.
- If the VLAN specified by the **vlan** argument is a dynamic VLAN, after a static MAC address is added, it will become a static VLAN.

Setting the Aging Time of MAC Address Entries

Setting aging time properly helps effective utilization of MAC address aging. The aging time that is too long or too short affects the performance of the device.

- If the aging time is too long, excessive invalid MAC address entries maintained by the device may fill up the MAC address table. This prevents the MAC address table from being updated with network changes in time.
- If the aging time is too short, the device may remove valid MAC address entries. This decreases the forwarding performance of the device.

Follow these steps to set the aging time of MAC address entries:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the aging time of MAC address entries	**mac-address timer** { **aging** *age* | **no-aging** }	Required The default aging time is 300 seconds.

Normally, you are recommended to use the default aging time, namely, 300 seconds. The **no-aging** keyword specifies that MAC address entries do not age out.

Note

MAC address aging configuration applies to all ports, but only takes effect on dynamic MAC addresses that are learnt or configured to age.

Setting the Maximum Number of MAC Addresses a Port Can Learn

The MAC address learning mechanism enables the device to acquire the MAC addresses of the network devices on the segment connected to the ports of the device. By searching the MAC address table, the device directly forwards the packets destined for these MAC addresses through the hardware, improving the forwarding efficiency. A MAC address table too big in size may prolong the time for searching MAC address entries, thus decreasing the forwarding performance of the device.

By setting the maximum number of MAC addresses that can be learned from individual ports, the administrator can control the number of the MAC address entries the MAC address table can dynamically maintain. When the number of the MAC address entries learnt from a port reaches the set value, the port stops learning MAC addresses.

Follow these steps to set the maximum number of MAC addresses a port can learn:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

To do…	Use the command…	Remarks
Set the maximum number of MAC addresses the port can learn	**mac-address max-mac-count** *count*	Required By default, the number of the MAC addresses a port can learn is not limited.

Note

Specifying the maximum number of MAC addresses a port can learn disables centralized MAC address authentication and port security on the port. On the other hand, if you enable centralized MAC address authentication and port security on a port, you cannot specify the maximum number of MAC addresses the port can learn.

Disabling MAC Address learning for a VLAN

You can disable a switch from learning MAC addresses in specific VLANs to improve stability and security for the users belong to these VLANs and prevent unauthorized accesses.

Follow these steps to disable MAC address learning for a VLAN:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	—
Disable the switch from learning MAC addresses in the VLAN	**mac-address max-mac-count** 0	Required By default, the device learns MAC addresses in every VLAN.

Note

- If the VLAN is configured as a remote probe VLAN used by port mirroring, you can not disable MAC address learning of this VLAN. Similarly, after you disable MAC address learning, this VLAN can not be configured as a remote probe VLAN.
- Disabling the MAC address learning function of a VLAN takes no effect on enabling the centralized MAC address authentication on the ports that belong to the VLAN.

Displaying and Maintaining MAC Address Table

To do…	Use the command…	Remarks
Display information about the MAC address table	**display mac-address** [*display-option*]	The **display** command can be executed in any view.
Display the aging time of the dynamic MAC address entries in the MAC address table	**display mac-address aging-time**	

Configuration Example

Adding a Static MAC Address Entry Manually

Network requirements

The server connects to the device through GigabitEthernet 1/0/2. To prevent the device from broadcasting packets destined for the server, it is required to add the MAC address of the server to the MAC address table of the device, which then forwards packets destined for the server through GigabitEthernet 1/0/2.

- The MAC address of the server is 000f-e20f-dc71.
- Port GigabitEthernet 1/0/2 belongs to VLAN 1.

Configuration procedure

Enter system view.

```
<device> system-view
```

Add a MAC address, with the VLAN, ports, and states specified.

```
[device] mac-address static 000f-e20f-dc71  interface GigabitEthernet 1/0/2 vlan 1
```

Display information about the current MAC address table.

```
[device] display mac-address interface GigabitEthernet 1/0/2
MAC ADDR         VLAN ID STATE           PORT INDEX           AGING TIME(s)
000f-e20f-dc71   1       Config static   GigabitEthernet1/0/2  NOAGED
000f-e20f-a7d6   1       Learned         GigabitEthernet1/0/2  AGING
000f-e20f-b1fb   1       Learned         GigabitEthernet1/0/2  AGING
000f-e20f-f116   1       Learned         GigabitEthernet1/0/2  AGING
---  4 mac address(es) found on port GigabitEthernet1/0/2 ---
```

Table of Contents

1 MSTP Configuration 1-1
STP Overview 1-1
STP Overview 1-1
MSTP Overview 1-9
Background of MSTP 1-9
Basic MSTP Terminologies 1-10
Principle of MSTP 1-13
MSTP Implementation on the Device 1-14
STP-related Standards 1-15
Configuring Root Bridge 1-15
Configuration Prerequisites 1-16
Configuring an MST Region 1-16
Specifying the Current Device as a Root Bridge/Secondary Root Bridge 1-17
Configuring the Bridge Priority of the Current Device 1-19
Configuring the Mode a Port Recognizes and Sends MSTP Packets 1-20
Configuring the MSTP Operation Mode 1-21
Configuring the Maximum Hop Count of an MST Region 1-22
Configuring the Network Diameter of the Switched Network 1-22
Configuring the MSTP Time-related Parameters 1-23
Configuring the Timeout Time Factor 1-24
Configuring the Maximum Transmitting Speed on the Current Port 1-25
Configuring the Current Port as an Edge Port 1-26
Specifying Whether the Link Connected to a Port Is Point-to-point Link 1-27
Enabling MSTP 1-28
Configuring Leaf Nodes 1-29
Configuration Prerequisites 1-30
Configuring the MST Region 1-30
Configuring the Mode a Port Recognizes and Sends MSTP Packets 1-30
Configuring the Timeout Time Factor 1-30
Configuring the Maximum Transmitting Speed on the Current Port 1-30
Configuring a Port as an Edge Port 1-30
Configuring the Path Cost for a Port 1-31
Configuring Port Priority 1-33
Specifying Whether the Link Connected to a Port Is a Point-to-point Link 1-34
Enabling MSTP 1-34
Performing mCheck Operation 1-34
Configuration Prerequisites 1-34
Configuration Procedure 1-34
Configuration Example 1-35
Configuring Guard Functions 1-35
Introduction 1-35
Configuration Prerequisites 1-37
Configuring BPDU Guard 1-37

Configuring Root Guard 1-37
Configuring Loop Guard 1-38
Configuring TC-BPDU Attack Guard 1-38
Configuring BPDU Dropping 1-39
Configuring Digest Snooping 1-39
Introduction 1-39
Configuring Digest Snooping 1-40
Configuring Rapid Transition 1-41
Introduction 1-41
Configuring Rapid Transition 1-43
Configuring VLAN-VPN Tunnel 1-44
Introduction 1-44
Configuring VLAN-VPN tunnel 1-44
STP Maintenance Configuration 1-45
Introduction 1-45
Enabling Log/Trap Output for Ports of MSTP Instance 1-45
Configuration Example 1-45
Enabling Trap Messages Conforming to 802.1d Standard 1-46
Displaying and Maintaining MSTP 1-46
MSTP Configuration Example 1-47
VLAN-VPN tunnel Configuration Example 1-49

1 MSTP Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

STP Overview

STP Overview

Functions of STP

Spanning tree protocol (STP) is a protocol conforming to IEEE 802.1d. It aims to eliminate loops on data link layer in a local area network (LAN). Devices running this protocol detect loops in the network by exchanging packets with one another and eliminate the loops detected by blocking specific ports until the network is pruned into one with tree topology. As a network with tree topology is loop-free, it prevents packets in it from being duplicated and forwarded endlessly and prevents device performance degradation.

Currently, in addition to the protocol conforming to IEEE 802.1d, STP also refers to the protocols based on IEEE 802.1d, such as RSTP, and MSTP.

Protocol packets of STP

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets.

STP identifies the network topology by transmitting BPDUs between STP compliant network devices. BPDUs contain sufficient information for the network devices to complete the spanning tree calculation.

In STP, BPDUs come in two types:

- Configuration BPDUs, used to calculate spanning trees and maintain the spanning tree topology.
- Topology change notification (TCN) BPDUs, used to notify concerned devices of network topology changes, if any.

Basic concepts in STP

1) Root bridge

A tree network must have a root; hence the concept of “root bridge” has been introduced in STP.

There is one and only one root bridge in the entire network, and the root bridge can change alone with changes of the network topology. Therefore, the root bridge is not fixed.

Upon network convergence, the root bridge generates and sends out configuration BPDUs periodically. Other devices just forward the configuration BPDUs received. This mechanism ensures the topological stability.

2) Root port

On a non-root bridge device, the root port is the port with the lowest path cost to the root bridge. The root port is used for communicating with the root bridge. A non-root-bridge device has one and only one root port. The root bridge has no root port.

3) Designated bridge and designated port

Refer to the following table for the description of designated bridge and designated port.

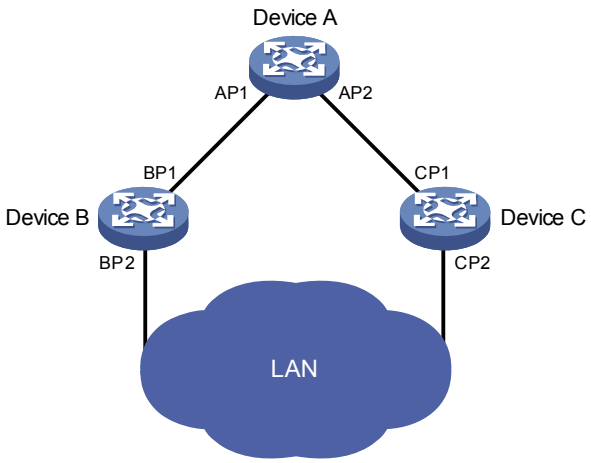
Table 1-1 Designated bridge and designated port

Classification	Designated bridge	Designated port
For a device	A designated bridge is a device that is directly connected to a WX3000 series device and is responsible for forwarding BPDUs to the device.	The port through which the designated bridge forwards BPDUs to this device
For a LAN	A designated bridge is a device responsible for forwarding BPDUs to this LAN segment.	The port through which the designated bridge forwards BPDUs to this LAN segment

Table 1-1 shows designated bridges and designated ports. In the figure, AP1 and AP2, BP1 and BP2, and CP1 and CP2 are ports on Device A, Device B, and Device C respectively.

- If Device A forwards BPDUs to Device B through AP1, the designated bridge for Device B is Device A, and the designated port is the port AP1 on Device A.
- Two devices are connected to the LAN: Device B and Device C. If Device B forwards BPDUs to the LAN, the designated bridge for the LAN is Device B, and the designated port is the port BP2 on Device B.

Figure 1-1 A schematic diagram of designated bridges and designated ports



Note

All the ports on the root bridge are designated ports.

4) Path cost

Path cost is a value used for measuring link capacity. By comparing the path costs of different links, STP selects the most robust links and blocks the other links to prune the network into a tree.

How STP works

STP identifies the network topology by transmitting configuration BPDUs between network devices. Configuration BPDUs contain sufficient information for network devices to complete the spanning tree calculation. Important fields in a configuration BPDU include:

- Root bridge ID, consisting of root bridge priority and MAC address.
- Root path cost, the cost of the shortest path to the root bridge.
- Designated bridge ID, designated bridge priority plus MAC address.
- Designated port ID, designated port priority plus port name.
- Message age: lifetime for the configuration BPDUs to be propagated within the network.
- Max age, lifetime for the configuration BPDUs to be kept in the device.
- Hello time, configuration BPDU interval.
- Forward delay, forward delay of the port.

 **Note**

For the convenience of description, the description and examples below involve only four parts of a configuration BPDU:

- Root bridge ID (in the form of device priority)
- Root path cost
- Designated bridge ID (in the form of device priority)
- Designated port ID (in the form of port name)

---

1) Detailed calculation process of the STP algorithm

- Initial state

Upon initialization of a device, each device generates a BPDU with itself as the root bridge, in which the root path cost is 0, designated bridge ID is the device ID, and the designated port is the local port.

- Selection of the optimum configuration BPDU

Each device sends out its configuration BPDU and receives configuration BPDUs from other devices.

The process of selecting the optimum configuration BPDU is as follows:

Table 1-2 Selection of the optimum configuration BPDU

Step	Description
1	Upon receiving a configuration BPDU on a port, the device performs the following processing: • If the received configuration BPDU has a lower priority than that of the configuration BPDU generated by the port, the device will discard the received configuration BPDU without doing any processing on the configuration BPDU of this port. • If the received configuration BPDU has a higher priority than that of the configuration BPDU generated by the port, the device will replace the content of the configuration BPDU generated by the port with the content of the received configuration BPDU.

Step	Description
2	The device compares the configuration BPDUs of all the ports and chooses the optimum configuration BPDU.

Note

Principle for configuration BPDU comparison:

- The configuration BPDU that has the lowest root bridge ID has the highest priority.
- If all the configuration BPDUs have the same root bridge ID, they will be compared for their root path costs. If the root path cost in a configuration BPDU plus the path cost corresponding to this port is S, the configuration BPDU with the smallest S value has the highest priority.
- If all configuration BPDUs have the same root path cost, the following configuration BPDU priority is compared sequentially: designated bridge IDs, designated port IDs, and then the IDs of the ports on which the configuration BPDUs are received. The device with a higher priority is elected as the root bridge.

- Selection of the root bridge

At network initialization, each STP-compliant device on the network assumes itself to be the root bridge, with the root bridge ID being its own bridge ID. By exchanging configuration BPDUs, the devices compare one another's root bridge ID. The device with the smallest root bridge ID is elected as the root bridge.

- Selection of the root port and designated ports

The process of selecting the root port and designated ports is as follows:

Table 1-3 Selection of the root port and designated ports

Step	Description
1	A non-root-bridge device takes the port on which the optimum configuration BPDU was received as the root port.
2	Based on the configuration BPDU and the path cost of the root port, the device calculates a designated port configuration BPDU for each of the rest ports. • The root bridge ID is replaced with that of the configuration BPDU of the root port. • The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost corresponding to the root port. • The designated bridge ID is replaced with the ID of this device. • The designated port ID is replaced with the ID of this port.
3	The device compares the calculated configuration BPDU with the configuration BPDU on the port whose role is to be determined, and acts as follows based on the comparison result: • If the calculated configuration BPDU is superior, this port will serve as the designated port, and the configuration BPDU on the port will be replaced with the calculated configuration BPDU, which will be sent out periodically. • If the configuration BPDU on the port is superior, the device stops updating the configuration BPDUs of the port and blocks the port, so that the port only receives configuration BPDUs, but does not forward data or send configuration BPDUs.

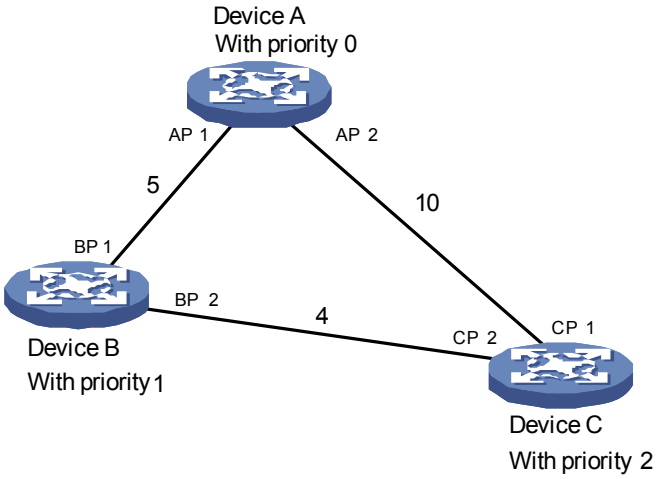
Note

When the network topology is stable, only the root port and designated ports forward traffic, while other ports are all in the blocked state – they only receive STP packets but do not forward user traffic.

Once the root bridge, the root port on each non-root bridge and designated ports have been successfully elected, the entire tree-shaped topology has been constructed.

The following is an example of how the STP algorithm works. The specific network diagram is shown in Figure 1-2. The priority of Device A is 0, the priority of Device B is 1, the priority of Device C is 2, and the path costs of these links are 5, 10 and 4 respectively.

Figure 1-2 Network diagram for STP algorithm



- Initial state of each device

The following table shows the initial state of each device.

Table 1-4 Initial state of each device

Device	Port name	BPDU of port
Device A	AP1	{0, 0, 0, AP1}
	AP2	{0, 0, 0, AP2}
Device B	BP1	{1, 0, 1, BP1}
	BP2	{1, 0, 1, BP2}
Device C	CP1	{2, 0, 2, CP1}
	CP2	{2, 0, 2, CP2}

- Comparison process and result on each device

The following table shows the comparison process and result on each device.

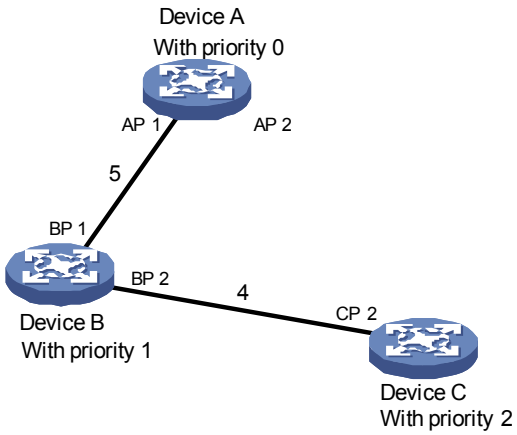
Table 1-5 Comparison process and result on each device

Device	Comparison process	BPDU of port after comparison
Device A	• Port AP1 receives the configuration BPDU of Device B {1, 0, 1, BP1}. Device A finds that the configuration BPDU of the local port {0, 0, 0, AP1} is superior to the configuration received message, and discards the received configuration BPDU. • Port AP2 receives the configuration BPDU of Device C {2, 0, 2, CP1}. Device A finds that the BPDU of the local port {0, 0, 0, AP2} is superior to the received configuration BPDU, and discards the received configuration BPDU. • Device A finds that both the root bridge and designated bridge in the configuration BPDUs of all its ports are Device A itself, so it assumes itself to be the root bridge. In this case, it does not make any change to the configuration BPDU of each port, and starts sending out configuration BPDUs periodically.	AP1: {0, 0, 0, AP1} AP2: {0, 0, 0, AP2}
Device B	• Port BP1 receives the configuration BPDU of Device A {0, 0, 0, AP1}. Device B finds that the received configuration BPDU is superior to the configuration BPDU of the local port {1, 0,1, BP1}, and updates the configuration BPDU of BP1. • Port BP2 receives the configuration BPDU of Device C {2, 0, 2, CP2}. Device B finds that the configuration BPDU of the local port {1, 0, 1, BP2} is superior to the received configuration BPDU, and discards the received configuration BPDU.	BP1: {0, 0, 0, AP1} BP2: {1, 0, 1, BP2}
	• Device B compares the configuration BPDUs of all its ports, and determines that the configuration BPDU of BP1 is the optimum configuration BPDU. Then, it uses BP1 as the root port, the configuration BPDUs of which will not be changed. • Based on the configuration BPDU of BP1 and the path cost of the root port (5), Device B calculates a designated port configuration BPDU for BP2 {0, 5, 1, BP2}. • Device B compares the calculated configuration BPDU {0, 5, 1, BP2} with the configuration BPDU of BP2. If the calculated BPDU is superior, BP2 will act as the designated port, and the configuration BPDU on this port will be replaced with the calculated configuration BPDU, which will be sent out periodically.	Root port BP1: {0, 0, 0, AP1} Designated port BP2: {0, 5, 1, BP2}

Device	Comparison process	BPDU of port after comparison
Device C	• Port CP1 receives the configuration BPDU of Device A {0, 0, 0, AP2}. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP1}, and updates the configuration BPDU of CP1. • Port CP2 receives the configuration BPDU of port BP2 of Device B {1, 0, 1, BP2} before the message was updated. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP2}, and updates the configuration BPDU of CP2.	CP1: {0, 0, 0, AP2} CP2: {1, 0, 1, BP2}
	By comparison: • The configuration BPDUs of CP1 is elected as the optimum configuration BPDU, so CP1 is identified as the root port, the configuration BPDUs of which will not be changed. • Device C compares the calculated designated port configuration BPDU {0, 10, 2, CP2} with the configuration BPDU of CP2, and CP2 becomes the designated port, and the configuration BPDU of this port will be replaced with the calculated configuration BPDU.	Root port CP1: {0, 0, 0, AP2} Designated port CP2: {0, 10, 2, CP2}
	• Next, port CP2 receives the updated configuration BPDU of Device B {0, 5, 1, BP2}. Because the received configuration BPDU is superior to its old one, Device C launches a BPDU update process. • At the same time, port CP1 receives configuration BPDUs periodically from Device A. Device C does not launch an update process after comparison.	CP1: {0, 0, 0, AP2} CP2: {0, 5, 1, BP2}
	By comparison: • Because the root path cost of CP2 (9) (root path cost of the BPDU (5) + path cost corresponding to CP2 (4)) is smaller than the root path cost of CP1 (10) (root path cost of the BPDU (0) + path cost corresponding to CP2 (10)), the BPDU of CP2 is elected as the optimum BPDU, and CP2 is elected as the root port, the messages of which will not be changed. • After comparison between the configuration BPDU of CP1 and the calculated designated port configuration BPDU, port CP1 is blocked, with the configuration BPDU of the port remaining unchanged, and the port will not receive data from Device A until a spanning tree calculation process is triggered by a new condition, for example, the link from Device B to Device C becomes down.	Blocked port CP2: {0, 0, 0, AP2} Root port CP2: {0, 5, 1, BP2}

After the comparison processes described in the table above, a spanning tree with Device A as the root bridge is stabilized, as shown in Figure 1-3.

Figure 1-3 The final calculated spanning tree



Note

To facilitate description, the spanning tree calculation process in this example is simplified, while the actual process is more complicated.

2) The BPDU forwarding mechanism in STP

- Upon network initiation, every device regards itself as the root bridge, generates configuration BPDUs with itself as the root, and sends the configuration BPDUs at a regular interval of hello time.
- If it is the root port that received the configuration BPDU and the received configuration BPDU is superior to the configuration BPDU of the port, the device will increase message age carried in the configuration BPDU by a certain rule and start a timer to time the configuration BPDU while it sends out this configuration BPDU through the designated port.
- If the configuration BPDU received on the designated port has a lower priority than the configuration BPDU of the local port, the port will immediately sends out its better configuration BPDU in response.
- If a path becomes faulty, the root port on this path will no longer receive new configuration BPDUs and the old configuration BPDUs will be discarded due to timeout. In this case, the device generates configuration BPDUs with itself as the root bridge and sends configuration BPDUs and TCN BPDUs. This triggers a new spanning tree calculation so that a new path is established to restore the network connectivity.

However, the newly calculated configuration BPDU will not be propagated throughout the network immediately, so the old root ports and designated ports that have not detected the topology change continue forwarding data through the old path. If the new root port and designated port begin to forward data as soon as they are elected, a temporary loop may occur.

3) STP timers

The following three time parameters are important for STP calculation:

- Forward delay, the period the device waits before state transition.

A link failure triggers a new round of spanning tree calculation and results in changes of the spanning tree. However, as new configuration BPDUs cannot be propagated throughout the network immediately, if the new root port and designated port begin to forward data as soon as they are elected, loops may temporarily occur.

For this reason, the protocol uses a state transition mechanism. Namely, a newly elected root port and the designated ports must go through a period, which is twice the forward delay time, before they transit to the forwarding state. The period allows the new configuration BPDUs to be propagated throughout the entire network.

- Hello time, the interval for sending hello packets. Hello packets are used to check link state.

The device sends hello packets to its neighboring devices at a regular interval (the hello time) to check whether the links are faulty.

- Max time, lifetime of the configuration BPDUs stored in the device. A configuration BPDU that has “expired” is discarded by the device.

MSTP Overview

Background of MSTP

Disadvantages of STP and RSTP

STP does not support rapid state transition of ports. A newly elected root port or designated port must wait twice the forward delay time before transiting to the forwarding state, even if it is a port on a point-to-point link or it is an edge port (an edge port refers to a port that directly connects to a user terminal rather than to another device or a shared LAN segment.)

The rapid spanning tree protocol (RSTP) is an optimized version of STP. RSTP allows a newly elected root port or designated port to enter the forwarding state much quicker under certain conditions than in STP. As a result, it takes a shorter time for the network to reach the final topology stability.



Note

- In RSTP, the state of a root port can transit fast under the following conditions: the old root port on the device has stopped forwarding data and the upstream designated port has started forwarding data.
- In RSTP, the state of a designated port can transit fast under the following conditions: the designated port is an edge port or a port connected with a point-to-point link. If the designated port is an edge port, it can enter the forwarding state directly; if the designated port is connected with a point-to-point link, it can enter the forwarding state immediately after the device undergoes handshake with the downstream device and gets a response.

RSTP supports rapid convergence. Like STP, it is of the following disadvantages: all bridges in a LAN are on the same spanning tree; redundant links cannot be blocked by VLAN; the packets of all VLANs are forwarded along the same spanning tree.

Features of MSTP

The multiple spanning tree protocol (MSTP) overcomes the shortcomings of STP and RSTP. In addition to support for rapid network convergence, it also allows data flows of different VLANs to be forwarded along their own paths, thus providing a better load sharing mechanism for redundant links.

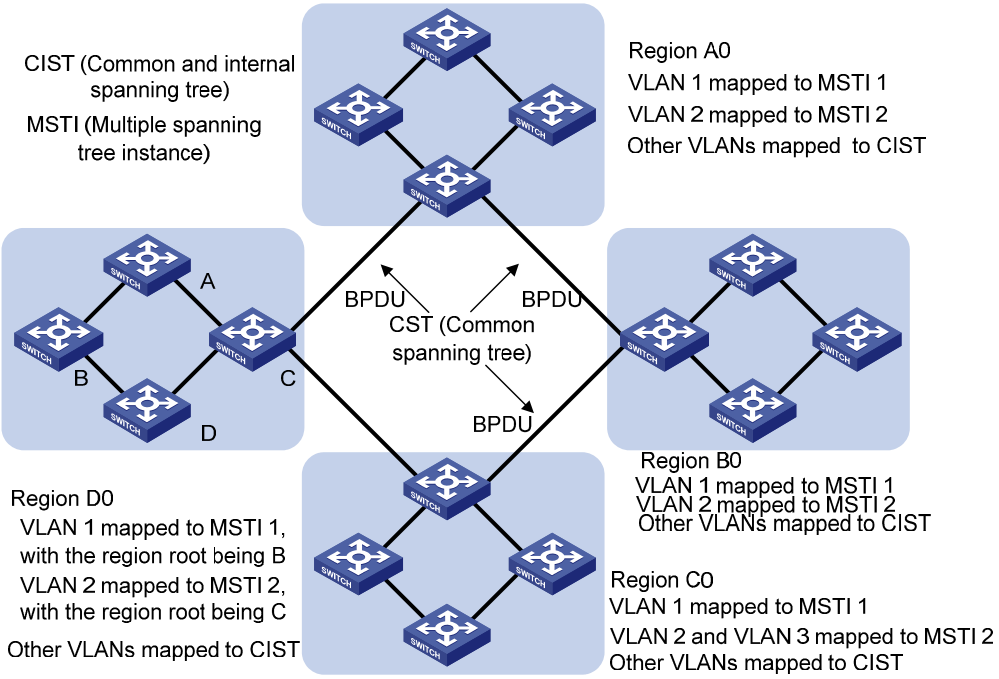
MSTP features the following:

- MSTP supports mapping VLANs to MST instances by means of a VLAN-to-instance mapping table. MSTP introduces “instance” (integrates multiple VLANs into a set) and can bind multiple VLANs to an instance, thus saving communication overhead and improving resource utilization.
- MSTP divides a switched network into multiple regions, each containing multiple spanning trees that are independent of one another.
- MSTP prunes a ring network into a network with tree topology, preventing packets from being duplicated and forwarded in a network endlessly. Furthermore, it offers multiple redundant paths for forwarding data, and thus achieves load balancing for forwarding VLAN data.
- MSTP is compatible with STP and RSTP.

Basic MSTP Terminologies

Figure 1-4 illustrates basic MSTP terms (assuming that MSTP is enabled on every device in this figure).

Figure 1-4 Basic MSTP terminologies



MST region

A multiple spanning tree region (MST region) comprises multiple physically-interconnected MSTP-enabled devices and the corresponding network segments connected to these devices. These devices have the same region name, the same VLAN-to-MSTI mapping configuration and the same MSTP revision level.

A switched network can contain multiple MST regions. You can group multiple devices into one MST region by using the corresponding MSTP configuration commands.

As shown in Figure 1-4, all the devices in region A0 are of the same MST region-related configuration, including:

- Region name
- VLAN-to-MSTI mapping (that is, VLAN 1 is mapped to MSTI 1, VLAN 2 is mapped to instance 2, and the other VLANs are mapped to CIST.)
- MSTP revision level (not shown in Figure 1-4)

MSTI

A multiple spanning tree instance (MSTI) refers to a spanning tree in an MST region.

Multiple spanning trees can be established in one MST region. These spanning trees are independent of each other. For example, each region in Figure 1-4 contains multiple spanning trees known as MSTIs. Each of these spanning trees corresponds to a VLAN.

VLAN mapping table

A VLAN mapping table is a property of an MST region. It contains information about how VLANs are mapped to MSTIs. For example, in Figure 1-4, the VLAN mapping table of region A0 is: VLAN 1 is mapped to MSTI 1; VLAN 2 is mapped to MSTI 2; and other VLANs are mapped to CIST. In an MST region, load balancing is implemented according to the VLAN mapping table.

IST

An internal spanning tree (IST) is a spanning tree in an MST region.

ISTs together with the common spanning tree (CST) form the common and internal spanning tree (CIST) of the entire switched network. An IST is a special MSTI; it is a branch of CIST in the MST region.

In Figure 1-4, each MST region has an IST, which is a branch of the CIST.

CST

A CST is a single spanning tree in a switched network that connects all MST regions in the network. If you regard each MST region in the network as a device, then the CST is the spanning tree generated by STP or RSTP running on the "devices".

CIST

A CIST is the spanning tree in a switched network that connects all devices in the network. It comprises the ISTs and the CST.

In Figure 1-4, the ISTs in the MST regions and the CST connecting the MST regions form the CIST.

Region root

A region root is the root of the IST or an MSTI in an MST region. Different spanning trees in an MST region may have different topologies and thus have different region roots.

In region D0 shown in Figure 1-4, the region root of MSTI 1 is Device B, and the region root of MSTI 2 is Device C.

Common root bridge

The common root bridge is the root of the CIST. The common root bridge of the network shown in Figure 1-4 is a device in region A0.

Port role

During MSTP calculation, the following port roles exist: root port, designated port, master port, region edge port, alternate port, and backup port.

- A root port is used to forward packets to the root.
- A designated port is used to forward packets to a downstream network segment or device.
- A master port connects an MST region to the common root. The path from the master port to the common root is the shortest path between the MST region and the common root.

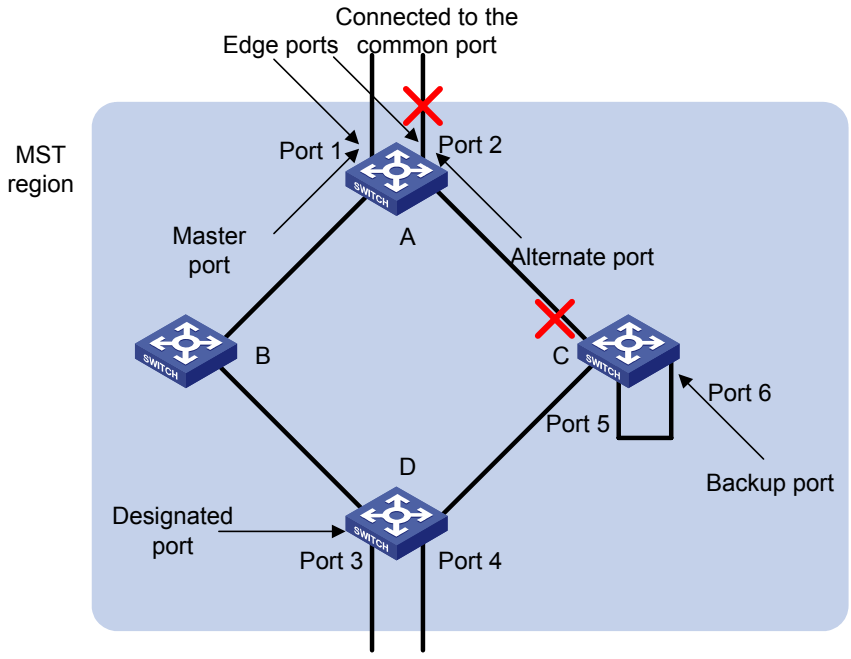
- A region edge port is located on the edge of an MST region and is used to connect one MST region to another MST region, an STP-enabled region or an RSTP-enabled region
- An alternate port is a secondary port of a root port or master port and is used for rapid transition. With the root port or master port being blocked, the alternate port becomes the new root port or master port.
- A backup port is the secondary port of a designated port and is used for rapid transition. With the designated port being blocked, the backup port becomes the new designated port fast and begins to forward data seamlessly. When two ports of an MSTP-enabled device are interconnected, the device blocks one of the two ports to eliminate the loop that occurs. The blocked port is the backup port.

In Figure 1-5, device A, device B, device C, and device D form an MST region. Port 1 and port 2 on device A connect upstream to the common root. Port 5 and port 6 on device C form a loop. Port 3 and port 4 on device D connect downstream to other MST regions. This figure shows the roles these ports play.

Note

- A port can play different roles in different MSTIs.
- The role a region edge port plays is consistent with the role it plays in the CIST. For example, port 1 on device A in Figure 1-5 is a region edge port, and it is a master port in the CIST. So it is a master port in all MSTIs in the region.

Figure 1-5 Port roles



Port state

In MSTP, a port can be in one of the following three states:

- Forwarding state. Ports in this state can forward user packets and receive/send BPDU packets.
- Learning state. Ports in this state can receive/send BPDU packets.
- Discarding state. Ports in this state can only receive BPDU packets.

Port roles and port states are not mutually dependent. Table 1-6 lists possible combinations of port states and port roles.

Table 1-6 Combinations of port states and port roles

Port role (right) / Port state (below)	Root/ port/Master port	Designated port	Region edge port	Alternate port	Backup port
Forwarding	√	√	√	—	—
Learning	√	√	√	—	—
Discarding	√	√	√	√	√

Principle of MSTP

MSTP divides a Layer 2 network into multiple MST regions. The CSTs are generated between these MST regions, and multiple spanning trees (also called MSTIs) can be generated in each MST region. As well as RSTP, MSTP uses configuration BPDUs for spanning tree calculation. The only difference is that the configuration BPDUs for MSTP carry the MSTP configuration information of the devices.

Calculate the CIST

Through comparing configuration BPDUs, the device with the highest priority in the network is selected as the root of the CIST. In each MST region, an IST is calculated by MSTP. At the same time, MSTP regards each MST region as a device to calculate the CSTs of the network. The CSTs, together with the ISTs, form the CIST of the network.

Calculate an MSTI

In an MST region, different MSTIs are generated for different VLANs based on the VLAN-to-MSTI mappings. Each spanning tree is calculated independently, in the same way as how STP/RSTP is calculated.

Implement STP algorithm

In the beginning, each device regards itself as the root, and generates a configuration BPDU for each port on it as a root, with the root path cost being 0, the ID of the designated bridge being that of the device, and the designated port being itself.

1) Each device sends out its configuration BPDUs and operates in the following way when receiving a configuration BPDU on one of its ports from another device:

- If the priority of the configuration BPDU is lower than that of the configuration BPDU of the port itself, the device discards the BPDU and does not change the configuration BPDU of the port.
- If the priority of the configuration BPDU is higher than that of the configuration BPDU of the port itself, the device replaces the configuration BPDU of the port with the received one and compares it with those of other ports on the device to obtain the one with the highest priority.

2) Configuration BPDUs are compared as follows:

For MSTP, CIST configuration information is generally expressed as follows:

(Root bridge ID, External path cost, Master bridge ID, Internal path cost, Designated bridge ID, ID of sending port, ID of receiving port), so the compared as follows

- The smaller the Root bridge ID of the configuration BPDU is, the higher the priority of the configuration BPDU is.
- For configuration BPDUs with the same Root bridge IDs, the External path costs are compared.
- For configuration BPDUs with both the same Root bridge ID and the same External path costs, Master bridge ID, Internal path cost, Designated bridge ID, ID of sending port, ID of receiving port are compared in turn.

For MSTP, MSTI configuration information is generally expressed as follows:

(Instance bridge ID, Internal path costs, Designated bridge ID, ID of sending port, ID of receiving port),so the compared as follows

- The smaller the Instance bridge ID of the configuration BPDU is, the higher the priority of the configuration BPDU is.
- For configuration BPDUs with the same Instance bridge IDs, Internal path costs are compared.
- For configuration BPDUs with both the same Instance bridge ID and the same Internal path costs, Designated bridge ID, ID of sending port, ID of receiving port are compared in turn.

3) A spanning tree is calculated as follows:

- Determining the root bridge

Root bridges are selected through the comparison of configuration BPDUs. The device with the smallest root ID is chosen as the root bridge.

- Determining the root port

For each device in a network, the port on which the configuration BPDU with the highest priority is received is chosen as the root port of the device.

- Determining the designated port

First, the device calculates a designated port configuration BPDU for each of its ports using the root port configuration BPDU and the root port path cost, with the root ID being replaced with that of the root port configuration BPDU, root path cost being replaced with the sum of the root path cost of the root port configuration BPDU and the path cost of the root port, the ID of the designated bridge being replaced with that of the device, and the ID of the designated port being replaced with that of the port.

The device then compares the calculated configuration BPDU with the original configuration BPDU received from the corresponding port on another device. If the latter takes precedence over the former, the device blocks the local port and keeps the port's configuration BPDU unchanged, so that the port can only receive configuration messages and cannot forward packets. Otherwise, the device sets the local port to the designated port, replaces the original configuration BPDU of the port with the calculated one and advertises it regularly.

MSTP Implementation on the Device

MSTP is compatible with both STP and RSTP. That is, an MSTP-enabled device can recognize the protocol packets of STP and RSTP and use them for spanning tree calculation. In addition to the basic MSTP functions, the device also provides the following functions for users to manage their devices.

- Root bridge hold
- Root bridge backup
- Root guard

- BPDU guard
- Loop guard
- TC-BPDU attack guard
- BPDU packet drop

STP-related Standards

STP-related standards include the following.

- IEEE 802.1D: spanning tree protocol
- IEEE 802.1w: rapid spanning tree protocol
- IEEE 802.1s: multiple spanning tree protocol

Configuring Root Bridge

Complete the following tasks to configure a root bridge:

Task	Remarks
Enabling MSTP	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after other related configurations are performed.
Configuring an MST Region	Required
Specifying the Current Device as a Root Bridge/Secondary Root Bridge	Required
Configuring the Bridge Priority of the Current Device	Optional The priority of a device cannot be changed after the device is specified as the root bridge or a secondary root bridge.
Configuring the Mode a Port Recognizes and Sends MSTP Packets	Optional
Configuring the MSTP Operation Mode	Optional
Configuring the Maximum Hop Count of an MST Region	Optional
Configuring the Network Diameter of the Switched Network	Optional The default value is recommended.
Configuring the MSTP Time-related Parameters	Optional The default values are recommended.
Configuring the Timeout Time Factor	Optional
Configuring the Maximum Transmitting Speed on the Current Port	Optional The default value is recommended.
Configuring the Current Port as an Edge Port	Optional
Specifying Whether the Link Connected to a Port Is Point-to-point Link	Optional

Note

In a network containing devices with both GVRP and MSTP enabled, GVRP packets are forwarded along the CIST. If you want to advertise packets of a specific VLAN through GVRP, be sure to map the VLAN to the CIST when configuring the MSTP VLAN mapping table (the CIST of a network is spanning tree instance 0).

Configuration Prerequisites

The role (root, branch, or leaf) of each device in each spanning tree instance is determined.

Configuring an MST Region

Configuration procedure

Follow these steps to configure an MST region:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter MST region view	**stp region-configuration**	—
Configure the name of the MST region	**region-name** *name*	Required The default MST region name of a device is its MAC address.
Configure the VLAN mapping table for the MST region	**instance** *instance-id* **vlan** *vlan-list*	Required Both commands can be used to configure VLAN mapping tables. By default, all VLANs in an MST region are mapped to spanning tree instance 0.
	vlan-mapping modulo *modulo*	
Configure the MSTP revision level for the MST region	**revision-level** *level*	Required The default revision level of an MST region is level 0.
Activate the configuration of the MST region manually	**active region-configuration**	Required
Display the configuration of the current MST region	**check region-configuration**	Optional
Display the currently valid configuration of the MST region	**display stp region-configuration**	You can execute this command in any view.

Note

NTDP packets sent by devices in a cluster can only be transmitted within the instance where the management VLAN of the cluster resides.

Configuring MST region-related parameters (especially the VLAN mapping table) results in spanning tree recalculation and network topology jitter. To reduce network topology jitter caused by the configuration, MSTP does not recalculate spanning trees immediately after the configuration; it does this only after you perform one of the following operations, and then the configuration can really takes effect:

- Activate the new MST region-related settings by using the **active region-configuration** command
- Enable MSTP by using the **stp enable** command

Note

Two devices belong to the same MST region only when they have the same MST region name, VLAN mapping table, and MSTP revision level.

Configuration example

Configure an MST region, with the name being “info”, the MSTP revision level being level 1, VLAN 2 through VLAN 10 being mapped to spanning tree instance 1, and VLAN 20 through VLAN 30 being mapped to spanning tree 2.

```
<device> system-view
[device] stp region-configuration
[device-mst-region] region-name info
[device-mst-region] instance 1 vlan 2 to 10
[device-mst-region] instance 2 vlan 20 to 30
[device-mst-region] revision-level 1
[device-mst-region] active region-configuration
```

Verify the above configuration.

```
[device-mst-region] check region-configuration
Admin configuration
   Format selector    :0
   Region name        :info
   Revision level     :1

   Instance   Vlans Mapped
      0       11 to 19, 31 to 4094
      1       1 to 10
      2       20 to 30
```

Specifying the Current Device as a Root Bridge/Secondary Root Bridge

MSTP can automatically choose a device as a root bridge through calculation. You can also manually specify the current device as a root bridge by using the corresponding commands.

Specify the current device as the root bridge of a spanning tree

Follow these steps to specify the current device as the root bridge of a spanning tree:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify the current device as the root bridge of a spanning tree	**stp** [**instance** *instance-id*] **root primary** [**bridge-diameter** *bridgenumber* [**hello-time** *centi-seconds*]]	Required

Specify the current device as the secondary root bridge of a spanning tree

Follow these steps to specify the current device as the secondary root bridge of a spanning tree:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify the current device as the secondary root bridge of a specified spanning tree	**stp** [**instance** *instance-id*] **root secondary** [**bridge-diameter** *bridgenumber* [**hello-time** *centi-seconds*]]	Required

Using the **stp root primary**/**stp root secondary** command, you can specify the current device as the root bridge or the secondary root bridge of the spanning tree instance identified by the *instance-id* argument. If the value of the *instance-id* argument is set to 0, the **stp root primary**/**stp root secondary** command specify the current device as the root bridge or the secondary root bridge of the CIST.

A device can play different roles in different spanning tree instances. That is, it can be the root bridges in a spanning tree instance and be a secondary root bridge in another spanning tree instance at the same time. But in the same spanning tree instance, a device cannot be the root bridge and the secondary root bridge simultaneously.

When the root bridge fails or is turned off, the secondary root bridge becomes the root bridge if no new root bridge is configured. If you configure multiple secondary root bridges for a spanning tree instance, the one with the smallest MAC address replaces the root bridge when the latter fails.

You can specify the network diameter and the hello time parameters while configuring a root bridge/secondary root bridge. Refer to Configuring the Network Diameter of the Switched Network and Configuring the MSTP Time-related Parameters for information about the network diameter parameter and the hello time parameter.

Note

- You can configure a device as the root bridges of multiple spanning tree instances. But you cannot configure two or more root bridges for one spanning tree instance. So, do not configure root bridges for the same spanning tree instance on two or more devices using the **stp root primary** command.
- You can configure multiple secondary root bridges for one spanning tree instance. That is, you can configure secondary root bridges for the same spanning tree instance on two or more devices using the **stp root secondary** command.
- You can also configure the current device as the root bridge by setting the priority of the device to 0. Note that once a device is configured as the root bridge or a secondary root bridge, its priority cannot be modified.

Configuration example

Configure the current device as the root bridge of spanning tree instance 1 and a secondary root bridge of spanning tree instance 2.

```
<device> system-view
[device] stp instance 1 root primary
[device] stp instance 2 root secondary
```

Configuring the Bridge Priority of the Current Device

Root bridges are selected according to the bridge priorities of the devices. You can make a specific device be selected as a root bridge by setting a lower bridge priority for it. An MSTP-enabled device can have different bridge priorities in different spanning tree instances.

Configuration procedure

Follow these steps to configure the bridge priority of the current device:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the bridge priority for the current device	**stp** [**instance** *instance-id*] **priority** *priority*	Required The default bridge priority of a device is 32,768.

Caution

- Once you specify a device as the root bridge or a secondary root bridge by using the **stp root primary** or **stp root secondary** command, the bridge priority of the device cannot be configured any more.
- During the selection of the root bridge, if multiple devices have the same bridge priority, the one with the smallest MAC address becomes the root bridge.

Configuration example

Set the bridge priority of the current device to 4,096 in spanning tree instance 1.

```
<device> system-view
[device] stp instance 1 priority 4096
```

Configuring the Mode a Port Recognizes and Sends MSTP Packets

A port can be configured to recognize and send MSTP packets in the following modes.

- Automatic mode. Ports in this mode determine the format of the MSTP packets to be sent according to the format of the received packets.
- Legacy mode. Ports in this mode recognize/send packets in legacy format.
- 802.1s mode. Ports in this mode recognize/send packets in dot1s format.

A port acts as follows according to the format of MSTP packets forwarded by a peer device or router.

When a port operates in the automatic mode:

- The port automatically determines the format (legacy or dot1s) of received MSTP packets and then determines the format of the packets to be sent accordingly, thus communicating with the peer devices.
- If the format of the received packets changes repeatedly, MSTP will shut down the corresponding port to prevent network storm. A port shut down in this way can only be brought up by the network administrator.

When a port operates in the legacy mode:

- The port only recognizes and sends MSTP packets in legacy format. In this case, the port can only communicate with the peer through packets in legacy format.
- If packets in dot1s format are received, the port turns to discarding state to prevent network storm.

When a port operates in the 802.1s mode:

- The port only recognizes and sends MSTP packets in dot1s format. In this case, the port can only communicate with the peer through packets in dot1s format.
- If packets in legacy format are received, the port turns to discarding state to prevent network storm.

Configuration procedure

Follow these steps to configure the mode a port recognizes and sends MSTP packets (in system view):

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the mode a port recognizes and sends MSTP packets	**stp interface** *interface-type interface-number* **compliance** { **auto** | **dot1s** | **legacy** }	Required By default, a port recognizes and sends MSTP packets in the automatic mode. That is, it determines the format of packets to be sent according to the format of the packets received.

Follow these steps to configure the mode a port recognizes and sends MSTP packets (in Ethernet port view):

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the mode a port recognizes and sends MSTP packets	**stp compliance** { **auto** | **dot1s** | **legacy** }	Required By default, a port recognizes and sends MSTP packets in the automatic mode. That is, it determines the format of packets to be sent according to the format of the packets received.

Configuration example

Configure GigabitEthernet 1/0/1 to recognize and send packets in dot1s format.

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] stp compliance dot1s
```

Restore the default mode for GigabitEthernet 1/0/1 to recognize/send MSTP packets.

```
[device-GigabitEthernet1/0/1] undo stp compliance
```

Configuring the MSTP Operation Mode

To make a MSTP-enabled device compatible with STP/RSTP, MSTP provides the following three operation modes:

- STP-compatible mode, where the ports of a device send STP BPDUs to neighboring devices. If STP-enabled devices exist in a switched network, you can use the **stp mode stp** command to configure an MSTP-enabled device to operate in STP-compatible mode.
- RSTP-compatible mode, where the ports of a device send RSTP BPDUs to neighboring devices. If RSTP-enabled devices exist in a switched network, you can use the **stp mode rstp** command to configure an MSTP-enabled device to operate in RSTP-compatible mode.
- MSTP mode, where the ports of a device send MSTP BPDUs or STP BPDUs (if the device is connected to STP-enabled devices) to neighboring devices. In this case, the device is MSTP-capable.

Configuration procedure

Follow these steps to configure the MSTP operation mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the MSTP operation mode	**stp mode** { **stp** | **rstp** | **mstp** }	Required An MSTP-enabled device operates in the MSTP mode by default.

Configuration example

Specify the MSTP operation mode as STP-compatible.

```
<device> system-view
[device] stp mode stp
```

Configuring the Maximum Hop Count of an MST Region

The maximum hop count configured on the region root is also the maximum hops of the MST region. The value of the maximum hop count limits the size of the MST region.

A configuration BPDU contains a field that maintains the remaining hops of the configuration BPDU. And the device discards the configuration BPDUs whose remaining hops are 0. After a configuration BPDU reaches a root bridge of a spanning tree in an MST region, the value of the remaining hops field in the configuration BPDU is decreased by 1 every time the configuration BPDU passes one device. Such a mechanism disables the devices that are beyond the maximum hop count from participating in spanning tree calculation, and thus limits the size of an MST region.

With such a mechanism, the maximum hop count configured on the device operating as the root bridge of the CIST or an MSTI in an MST region becomes the network diameter of the spanning tree, which limits the size of the spanning tree in the current MST region. The devices that are not root bridges in the MST region adopt the maximum hop settings of their root bridges.

Configuration procedure

Follow these steps to configure the maximum hop count for an MST region:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the maximum hop count of the MST region	**stp max-hops** *hops*	Required By default, the maximum hop count of an MST region is 20.

The bigger the maximum hop count, the larger the MST region is. Note that only the maximum hop settings on the device operating as a region root can limit the size of the MST region.

Configuration example

Configure the maximum hop count of the MST region to be 30.

```
<device> system-view
[device] stp max-hops 30
```

Configuring the Network Diameter of the Switched Network

In a switched network, any two devices can communicate with each other through a specific path made up of multiple devices. The network diameter of a network is measured by the number of devices; it equals the number of the devices on the longest path (that is, the path containing the maximum number of devices).

Configuration procedure

Follow these steps to configure the network diameter of the switched network:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the network diameter of the switched network	**stp bridge-diameter** *bridgenumber*	Required The default network diameter of a network is 7.

The network diameter parameter indicates the size of a network. The bigger the network diameter is, the larger the network size is.

After you configure the network diameter of a switched network, an MSTP-enabled device adjusts its hello time, forward delay, and max age settings accordingly to better values.

The network diameter setting only applies to CIST; it is invalid for MSTIs.

Configuration example

Configure the network diameter of the switched network to 6.

```
<device> system-view
[device] stp bridge-diameter 6
```

Configuring the MSTP Time-related Parameters

Three MSTP time-related parameters exist: forward delay, hello time, and max age. You can configure the three parameters to control the process of spanning tree calculation.

Configuration procedure

Follow these steps to configure MSTP time-related parameters:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the forward delay parameter	**stp timer forward-delay** *centiseconds*	Required The forward delay parameter defaults to 1,500 centiseconds (namely, 15 seconds).
Configure the hello time parameter	**stp timer hello** *centiseconds*	Required The hello time parameter defaults to 200 centiseconds (namely, 2 seconds).
Configure the max age parameter	**stp timer max-age** *centiseconds*	Required The max age parameter defaults to 2,000 centiseconds (namely, 20 seconds).

All devices in a switched network adopt the three time-related parameters configured on the CIST root bridge.

Caution

- The forward delay parameter and the network diameter are correlated. Normally, a large network diameter corresponds to a large forward delay. A too small forward delay parameter may result in temporary redundant paths. And a too large forward delay parameter may cause a network unable to resume the normal state in time after changes occurred to the network. The default value is recommended.
- An adequate hello time parameter enables a device to detect link failures in time without occupying too many network resources. And a too small hello time parameter may result in duplicated configuration BPDUs being sent frequently, which increases the work load of the devices and wastes network resources. The default value is recommended.
- As for the max age parameter, if it is too small, network congestion may be falsely regarded as link failures, which results in frequent spanning tree recalculation. If it is too large, link problems may be unable to be detected in time, which prevents spanning trees being recalculated in time and makes the network less adaptive. The default value is recommended.

As for the configuration of the three time-related parameters (that is, the hello time, forward delay, and max age parameters), the following formulas must be met to prevent frequent network jitter.

2 x (forward delay – 1 second) >= max age

Max age >= 2 x (hello time + 1 second)

You are recommended to specify the network diameter of the switched network and the hello time by using the **stp root primary** or **stp root secondary** command. After that, the three proper time-related parameters are determined automatically.

Configuration example

Configure the forward delay parameter to be 1,600 centiseconds, the hello time parameter to be 300 centiseconds, and the max age parameter to be 2,100 centiseconds (assuming that the current device operates as the CIST root bridge).

```
<device> system-view
[device] stp timer forward-delay 1600
[device] stp timer hello 300
[device] stp timer max-age 2100
```

Configuring the Timeout Time Factor

When the network topology is stable, a non-root-bridge device regularly forwards BPDUs received from the root bridge to its neighboring devices at the interval specified by the hello time parameter to check link failures. Normally, a device regards its upstream device faulty if the former does not receive any BPDU from the latter in a period three times of the hello time and then initiates the spanning tree recalculation process.

Spanning trees may be recalculated even in a steady network if an upstream device continues to be busy. You can configure the timeout time factor to a larger number to avoid such cases. Normally, the timeout time can be four or more times of the hello time. For a steady network, the timeout time can be five to seven times of the hello time.

Configuration procedure

Follow these steps to configure the timeout time factor:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the timeout time factor for the device	**stp timer-factor** *number*	Required The timeout time factor defaults to 3.

For a steady network, the timeout time can be five to seven times of the hello time.

Configuration example

Configure the timeout time factor to be 6.

```
<device> system-view
[device] stp timer-factor 6
```

Configuring the Maximum Transmitting Speed on the Current Port

The maximum transmitting speed of a port specifies the maximum number of configuration BPDUs a port can transmit in a period specified by the hello time parameter. It depends on the physical state of the port and network structure. You can configure this parameter according to the network.

Configure the maximum transmitting speed for specified ports in system view

Follow these steps to configure the maximum transmitting speed for specified ports in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the maximum transmitting speed for specified ports	**stp interface** *interface-list* **transmit-limit** *packetnum*	Required The maximum transmitting speed of all Ethernet ports on a device defaults to 10.

Configure the maximum transmitting speed in Ethernet port view

Follow these steps to configure the maximum transmitting speed in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the maximum transmitting speed	**stp transmit-limit** *packetnum*	Required The maximum transmitting speed of all Ethernet ports on a device defaults to 10.

As the maximum transmitting speed parameter determines the number of the configuration BPDUs transmitted in each hello time, set it to a proper value to prevent MSTP from occupying too many network resources. The default value is recommended.

Configuration example

Set the maximum transmitting speed of GigabitEthernet 1/0/1 to 15.

1) Configure the maximum transmitting speed in system view

```
<device> system-view
[device] stp interface GigabitEthernet1/0/1 transmit-limit 15
```

2) Configure the maximum transmitting speed in Ethernet port view

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] stp transmit-limit 15
```

Configuring the Current Port as an Edge Port

Edge ports are ports that neither directly connects to other devices nor indirectly connects to other devices through network segments. After a port is configured as an edge port, the rapid transition mechanism is applicable to the port. That is, when the port changes from the blocking state to the forwarding state, it does not have to wait for a delay.

You can configure a port as an edge port in one of the following two ways.

Configure a port as an edge port in system view

Follow these steps to configure a port as an edge port in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the specified ports as edge ports	**stp interface** *interface-list* **edged-port enable**	Required By default, all the Ethernet ports of a device are non-edge ports.

Configure a port as an edge port in Ethernet port view

Follow these steps to configure a port as an edge port in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the port as an edge port	**stp edged-port enable**	Required By default, all the Ethernet ports of a device are non-edge ports.

On a device with BPDU guard disabled, an edge port becomes a non-edge port again once it receives a BPDU from another port.

Note

You are recommended to configure the Ethernet ports connected directly to terminals as edge ports and enable the BPDU guard function at the same time. This not only enables these ports to turn to the forwarding state rapidly but also secures your network.

Configuration example

Configure GigabitEthernet 1/0/1 as an edge port.

1) Configure GigabitEthernet1/0/1 as an edge port in system view

```
<device> system-view
[device] stp interface GigabitEthernet1/0/1 edged-port enable
```

2) Configure GigabitEthernet 1/0/1 as an edge port in Ethernet port view

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] stp edged-port enable
```

Specifying Whether the Link Connected to a Port Is Point-to-point Link

A point-to-point link directly connects two devices. If the roles of the two ports at the two ends of a point-to-point link meet certain criteria, the two ports can turn to the forwarding state rapidly by exchanging synchronization packets, thus reducing the forward delay.

You can determine whether or not the link connected to a port is a point-to-point link in one of the following two ways.

Specify whether the link connected to a port is point-to-point link in system view

Follow these steps to specify whether the link connected to a port is point-to-point link in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify whether the link connected to a port is point-to-point link	**stp interface** *interface-list* **point-to-point** { **force-true** | **force-false** | **auto** }	Required The **auto** keyword is adopted by default.

Specify whether the link connected to a port is point-to-point link in Ethernet port view

Follow these steps to specify whether the link connected to a port is point-to-point link in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

To do…	Use the command…	Remarks
Specify whether the link connected to a port is a point-to-point link	**stp point-to-point** { **force-true** | **force-false** | **auto** }	Required The **auto** keyword is adopted by default.

Note

- Among aggregated ports, you can only configure the links of master ports as point-to-point links.
- If an auto-negotiating port operates in full duplex mode after negotiation, you can configure the link of the port as a point-to-point link.

After you configure the link of a port as a point-to-point link, the configuration applies to all the spanning tree instances the port belongs to. If the actual physical link of a port is not a point-to-point link and you forcibly configure the link as a point-to-point link, loops may occur temporarily.

Configuration example

Configure the link connected to GigabitEthernet 1/0/1 as a point-to-point link.

1) Perform this configuration in system view

```
<device> system-view
[device] stp interface GigabitEthernet1/0/1 point-to-point force-true
```

2) Perform this configuration in Ethernet port view

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] stp point-to-point force-true
```

Enabling MSTP

Configuration procedure

Follow these steps to enable MSTP in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable MSTP	**stp enable**	Required MSTP is disabled by default.
Disable MSTP on specified ports	**stp interface** *interface-list* **disable**	Optional By default, MSTP is enabled on all ports after you enable MSTP in system view. To enable a device to operate more flexibly, you can disable MSTP on specific ports. As MSTP-disabled ports do not participate in spanning tree calculation, this operation saves CPU resources of the device.

Follow these steps to enable MSTP in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable MSTP	**stp enable**	Required MSTP is disabled by default.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Disable MSTP on the port	**stp disable**	Optional By default, MSTP is enabled on all ports after you enable MSTP in system view. To enable a device to operate more flexibly, you can disable MSTP on specific ports. As MSTP-disabled ports do not participate in spanning tree calculation, this operation saves CPU resources of the device.



Note

You are not recommended to enable MSTP on GigabitEthernet 1/0/29 on the switching engine of the WX3024, GigabitEthernet 1/0/11 on the switching engine of the WX3010 or GigabitEthernet 1/0/9 on the switching engine of the WX3008.

Other MSTP-related settings can take effect only after MSTP is enabled on the device.

Configuration example

Enable MSTP on the device and disable MSTP on GigabitEthernet 1/0/1.

1) Perform this configuration in system view

```
<device> system-view
[device] stp enable
[device] stp interface GigabitEthernet1/0/1 disable
```

2) Perform this configuration in Ethernet port view

```
<device> system-view
[device] stp enable
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] stp disable
```

Configuring Leaf Nodes

Complete the following tasks to configure a leaf node:

Task	Remarks
Enabling MSTP	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after performing other configurations.
Configuring an MST Region	Required

Task	Remarks
Configuring the Mode a Port Recognizes and Sends MSTP Packets	Optional
Configuring the Timeout Time Factor	Optional
Configuring the Maximum Transmitting Speed on the Current Port	Optional The default value is recommended.
Configuring the Current Port as an Edge Port	Optional
Configuring the Path Cost for a Port	Optional
Configuring Port Priority	Optional
Specifying Whether the Link Connected to a Port Is Point-to-point Link	Optional



Note

In a network containing devices with both GVRP and MSTP enabled, GVRP packets are forwarded along the CIST. In this case, if you want to broadcast packets of a specific VLAN through GVRP, be sure to map the VLAN to the CIST when configuring the MSTP VLAN mapping table (the CIST of a network is spanning tree instance 0).

Configuration Prerequisites

The role (root, branch, or leaf) of each device in each spanning tree instance is determined.

Configuring the MST Region

Refer to Configuring an MST Region.

Configuring the Mode a Port Recognizes and Sends MSTP Packets

Refer to Configuring the Mode a Port Recognizes and Sends MSTP Packets.

Configuring the Timeout Time Factor

Refer to Configuring the Timeout Time Factor.

Configuring the Maximum Transmitting Speed on the Current Port

Refer to Configuring the Maximum Transmitting Speed on the Current Port.

Configuring a Port as an Edge Port

Refer to Configuring the Current Port as an Edge Port.

Configuring the Path Cost for a Port

The path cost parameter reflects the rate of the link connected to the port. For a port on an MSTP-enabled device, the path cost may be different in different spanning tree instances. You can enable flows of different VLANs to travel along different physical links by configuring appropriate path costs on ports, so that VLAN-based load balancing can be implemented.

Path cost of a port can be determined by the device or through manual configuration.

Standards for calculating path costs of ports

Currently, the device can calculate the path costs of ports based on one of the following standards:

- **dot1d-1998**: Adopts the IEEE 802.1D-1998 standard to calculate the default path costs of ports.
- **dot1t**: Adopts the IEEE 802.1t standard to calculate the default path costs of ports.
- **legacy**: Adopts the proprietary standard to calculate the default path costs of ports.

Follow these steps to specify the standard for calculating path costs:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify the standard for calculating the default path costs of the links connected to the ports of the device	**stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }	Optional By default, the legacy standard is used to calculate the default path costs of ports.

Table 1-7 Transmission speeds and the corresponding path costs

Transmission speed	Operation mode (half-/full-duplex)	802.1D-1998	IEEE 802.1t	Proprietary standard
0	—	65,535	200,000,000	200,000
10 Mbps	Half-duplex/Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	100 95 95 95	200,000 1,000,000 666,666 500,000	2,000 1,800 1,600 1,400
100 Mbps	Half-duplex/Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	19 15 15 15	200,000 100,000 66,666 50,000	200 180 160 140
1,000 Mbps	Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	4 3 3 3	200,000 10,000 6,666 5,000	20 18 16 14
10 Gbps	Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	2 1 1 1	200,000 1,000 666 500	2 1 1 1

Normally, the path cost of a port operating in full-duplex mode is slightly less than that of the port operating in half-duplex mode.

When calculating the path cost of an aggregated link, the 802.1D-1998 standard does not take the number of the ports on the aggregated link into account, whereas the 802.1T standard does. The following formula is used to calculate the path cost of an aggregated link:

Path cost = 200,000/ link transmission speed,

where ‘link transmission speed” is the sum of the speeds of all the unblocked ports on the aggregated link measured in 100 Kbps.

Configure the path cost for specific ports

Follow these steps to configure the path cost for specified ports in system view:

To do…	Use the command…	Remarks
Enter system view	**System-view**	—
Configure the path cost for specified ports	**stp interface** *interface-list* [**instance** *instance-id*] **cost** *cost*	Required An MSTP-enabled device can calculate path costs for all its ports automatically.

Follow these steps to configure the path cost for a port in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**System-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the path cost for the port	**stp** [**instance** *instance-id*] **cost** *cost*	Required An MSTP-enabled device can calculate path costs for all its ports automatically.

Changing the path cost of a port may change the role of the port and put it in state transition. Executing the **stp cost** command with the *instance-id* argument being 0 sets the path cost on the CIST for the port.

Configuration example (A)

Configure the path cost of GigabitEthernet 1/0/1 in spanning tree instance 1 to be 2,000.

1) Perform this configuration in system view

```
<device> system-view
[device] stp interface GigabitEthernet1/0/1 instance 1 cost 2000
```

2) Perform this configuration in Ethernet port view

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] stp instance 1 cost 2000
```

Configuration example (B)

Configure the path cost of GigabitEthernet 1/0/1 in spanning tree instance 1 to be calculated by the MSTP-enabled device according to the IEEE 802.1D-1998 standard.

1) Perform this configuration in system view

```
<device> system-view
[device] undo stp interface GigabitEthernet1/0/1 instance 1 cost
```

```
[device] stp pathcost-standard dot1d-1998
```

2) Perform this configuration in Ethernet port view

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] undo stp instance 1 cost
[device-GigabitEthernet1/0/1] quit
[device] stp pathcost-standard dot1d-1998
```

Configuring Port Priority

Port priority is an important criterion on determining the root port. In the same condition, the port with the smallest port priority value becomes the root port.

A port on an MSTP-enabled device can have different port priorities and play different roles in different spanning tree instances. This enables packets of different VLANs to be forwarded along different physical paths, so that VLAN-based load balancing can be implemented.

You can configure port priority in one of the following two ways.

Configure port priority in system view

Follow these steps to configure port priority in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure port priority for specified ports	**stp interface** *interface-list* **instance** *instance-id* **port priority** *priority*	Required The default port priority is 128.

Configure port priority in Ethernet port view

Follow these steps to configure port priority in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure port priority for the port	**stp** [**instance** *instance-id*] **port priority** *priority*	Required. The default port priority is 128.

Changing port priority of a port may change the role of the port and put the port into state transition.

A smaller port priority value indicates a higher possibility for the port to become the root port. If all the ports of a device have the same port priority value, the port priorities are determined by the port indexes. Changing the priority of a port will cause spanning tree recalculation.

You can configure port priorities according to actual networking requirements.

Configuration example

Configure the port priority of GigabitEthernet 1/0/1 in spanning tree instance 1 to be 16.

1) Perform this configuration in system view

```
<device> system-view
```

```
[device] stp interface GigabitEthernet1/0/1 instance 1 port priority 16
```

2) Perform this configuration in Ethernet port view

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] stp instance 1 port priority 16
```

Specifying Whether the Link Connected to a Port Is a Point-to-point Link

Refer to Specifying Whether the Link Connected to a Port Is Point-to-point Link.

Enabling MSTP

Refer to Enabling MSTP.

Performing mCheck Operation

Ports on an MSTP-enabled device can operate in three modes: STP-compatible, RSTP-compatible, and MSTP.

A port on an MSTP-enabled device operating as an upstream device transits to the STP-compatible mode when it has an STP-enabled device connected to it. When the STP-enabled downstream device is then replaced by an MSTP-enabled device, the port cannot automatically transit to the MSTP mode. It remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP mode by performing the mCheck operation on the port.

Similarly, a port on an RSTP-enabled device operating as an upstream device turns to the STP-compatible mode when it has an STP-enabled device connected to it. When the STP enabled downstream device is then replaced by an MSTP-enabled device, the port cannot automatically transit to the RSTP mode. It remains in the STP-compatible mode. In this case, you can force the port to transit to the RSTP mode by performing the mCheck operation on the port.

Configuration Prerequisites

MSTP runs normally on the device.

Configuration Procedure

You can perform the mCheck operation in the following two ways.

Perform the mCheck operation in system view

Follow these steps to perform the mCheck operation in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Perform the mCheck operation	**stp** [**interface** *interface-list*] **mcheck**	Required

Perform the mCheck operation in Ethernet port view

Follow these steps to perform the mCheck operation in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Perform the mCheck operation	**stp mcheck**	Required

Configuration Example

Perform the mCheck operation on GigabitEthernet 1/0/1.

1) Perform this configuration in system view

```
<device> system-view
[device] stp interface GigabitEthernet1/0/1 mcheck
```

2) Perform this configuration in Ethernet port view

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] stp mcheck
```

Configuring Guard Functions

Introduction

The following guard functions are available on an MSTP-enabled device: BPDU guard, root guard, loop guard, TC-BPDU attack guard, and BPDU drop.

BPDU guard

Normally, the access ports of the devices operating on the access layer are directly connected to terminals (such as PCs) or file servers. These ports are usually configured as edge ports to achieve rapid transition. But they resume non-edge ports automatically upon receiving configuration BPDUs, which causes spanning tree recalculation and network topology jitter.

Normally, no configuration BPDU will reach edge ports. But malicious users can attack a network by sending configuration BPDUs deliberately to edge ports to cause network jitter. You can prevent this type of attacks by utilizing the BPDU guard function. With this function enabled on a device, the device shuts down the edge ports that receive configuration BPDUs and then reports these cases to the administrator. Ports shut down in this way can only be restored by the administrator.

Root guard

A root bridge and its secondary root bridges must reside in the same region. The root bridge of the CIST and its secondary root bridges are usually located in the high-bandwidth core region. Configuration errors or attacks may result in configuration BPDUs with their priorities higher than that of a root bridge, which causes a new root bridge to be elected and network topology jitter to occur. In this case, flows that should travel along high-speed links may be led to low-speed links, and network congestion may occur.

You can avoid this problem by utilizing the root guard function. Ports with this function enabled can only be kept as designated ports in all spanning tree instances. When a port of this type receives configuration BPDUs with higher priorities, it turns to the discarding state (rather than become a non-designated port) and stops forwarding packets (as if it is disconnected from the link). It resumes the normal state if it does not receive any configuration BPDUs with higher priorities for a specified period.

Loop guard

A device maintains the states of the root port and other blocked ports by receiving and processing BPDUs from the upstream device. These BPDUs may get lost because of network congestions or unidirectional link failures. If a device does not receive BPDUs from the upstream device for certain period, the device selects a new root port; the original root port becomes a designated port; and the blocked ports turns to the forwarding state. This may cause loops in the network.

The loop guard function suppresses loops. With this function enabled, if link congestions or unidirectional link failures occur, both the root port and the blocked ports become designated ports and turn to the discarding state. In this case, they stop forwarding packets, and thereby loops can be prevented.

Caution

With the loop guard function enabled, the root guard function and the edge port configuration are mutually exclusive.

TC-BPDU attack guard

Normally, a device removes its MAC address table and ARP entries upon receiving TC-BPDUs. If a malicious user sends a large amount of TC-BPDUs to a device in a short period, the device may be busy in removing the MAC address table and ARP entries, which may affect spanning tree calculation, occupy large amount of bandwidth and increase device CPU utilization.

With the TC-BPDU attack guard function enabled, a device performs a removing operation upon receiving a TC-BPDU and triggers a timer (set to 10 seconds by default) at the same time. Before the timer expires, the device only performs the removing operation for limited times (up to six times by default) regardless of the number of the TC-BPDUs it receives. Such a mechanism prevents a device from being busy in removing the MAC address table and ARP entries.

You can use the **stp tc-protection threshold** command to set the maximum times for a device to remove the MAC address table and ARP entries in a specific period. When the number of the TC-BPDUs received within a period is less than the maximum times, the device performs a removing operation upon receiving a TC-BPDU. After the number of the TC-BPDUs received reaches the maximum times, the device stops performing the removing operation. For example, if you set the maximum times for a device to remove the MAC address table and ARP entries to 100 and the device receives 200 TC-BPDUs in the period, the device removes the MAC address table and ARP entries for only 100 times within the period.

BPDU dropping

In a STP-enabled network, some users may send BPDU packets to the device continuously in order to destroy the network. When a device receives the BPDU packets, it will forward them to other devices. As a result, STP calculation is performed repeatedly, which may occupy too much CPU of the devices or cause errors in the protocol state of the BPDU packets.

In order to avoid this problem, you can enable BPDU dropping on Ethernet ports. Once the function is enabled on a port, the port will not receive or forward any BPDU packets. In this way, the device is protected against the BPDU packet attacks so that the STP calculation is assured to be right.

Configuration Prerequisites

MSTP runs normally on the device.

Configuring BPDU Guard

Configuration procedure

Follow these steps to configure BPDU guard:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the BPDU guard function	**stp bpdu-protection**	Required The BPDU guard function is disabled by default.

Configuration example

Enable the BPDU guard function.

```
<device> system-view
[device] stp bpdu-protection
```

Configuring Root Guard

Configuration procedure

Follow these steps to configure the root guard function in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the root guard function on specified ports	**stp interface** *interface-list* **root-protection**	Required The root guard function is disabled by default.

Follow these steps to enable the root guard function in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**Interface** *interface-type interface-number*	—
Enable the root guard function on the current port	**stp root-protection**	Required The root guard function is disabled by default.

Configuration example

Enable the root guard function on GigabitEthernet 1/0/1.

1) Perform this configuration in system view

```
<device> system-view
[device] stp interface GigabitEthernet1/0/1 root-protection
```

2) Perform this configuration in Ethernet port view

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] stp root-protection
```

Configuring Loop Guard

Configuration procedure

Follow these steps to configure loop guard:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the loop guard function on the current port	**stp loop-protection**	Required The loop guard function is disabled by default.

Configuration example

Enable the loop guard function on GigabitEthernet 1/0/1.

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] stp loop-protection
```

Configuring TC-BPDU Attack Guard

Configuration prerequisites

MSTP runs normally on the device.

Configuration procedure

Follow these steps to configure the TC-BPDU attack guard function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the TC-BPDU attack guard function	**stp tc-protection enable**	Required The TC-BPDU attack guard function is disabled by default.
Set the maximum times that a device can remove the MAC address table within each 10 seconds	**stp tc-protection threshold** *number*	Optional

Configuration example

Enable the TC-BPDU attack guard function

```
<device> system-view
[device] stp tc-protection enable
```

Set the maximum times for the device to remove the MAC address table within 10 seconds to 5.

```
<device> system-view
[device] stp tc-protection threshold 5
```

Configuring BPDU Dropping

Follow these steps to configure BPDU dropping:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-name*	—
Enable BPDU dropping	**bpdu-drop any**	Required BPDU dropping is disabled by default.

Enable BPDU dropping on GigabitEthernet 1/0/1.

```
<device>system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] bpdu-drop any
```

Configuring Digest Snooping

Introduction

According to IEEE802.1s, two interconnected devices can communicate with each other through MSTIs in an MST region only when the two devices have the same MST region-related configuration. Interconnected MSTP-enabled devices determine whether or not they are in the same MST region by checking the configuration IDs of the BPDUs between them. (A configuration ID contains information such as region ID and configuration digest.)

As some other vendors' devices adopt proprietary spanning tree protocols, they cannot communicate with the other devices in an MST region even if they are configured with the same MST region-related settings as the other devices in the MST region.

This problem can be solved by implementing the digest snooping feature. If a port on a device is connected to another vendor's device that has the same MST region-related configuration as its own but adopts a proprietary spanning tree protocol, you can enable digest snooping on the port. Then the device regards devices of another manufacturer as in the same region; it records the configuration digests carried in the BPDUs received from the devices of another vendor, and put them in the BPDUs to be sent to these devices. In this way, the device can communicate with the devices of another vendor in the same MST region.

Caution

The digest snooping function is not applicable to edge ports.

Configuring Digest Snooping

Configure the digest snooping feature on a device to enable it to communicate with other devices adopting proprietary protocols to calculate configuration digests in the same MST region through MSTIs.

Configuration prerequisites

The device to be configured is connected to a device of another vendor adopting a proprietary spanning tree protocol. MSTP and the network operate normally.

Configuration procedure

Follow these steps to configure digest snooping:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the digest snooping feature	**stp config-digest-snooping**	Required The digest snooping feature is disabled on a port by default.
Return to system view	**quit**	—
Enable the digest snooping feature globally	**stp config-digest-snooping**	Required The digest snooping feature is disabled globally by default.
Display the current configuration	**display current-configuration**	You can execute this command in any view.

Note

- When the digest snooping feature is enabled on a port, the port state turns to the discarding state. That is, the port will not send BPDU packets. The port is not involved in the STP calculation until it receives BPDU packets from the peer port.
- The digest snooping feature is needed only when your device is connected to a device of another vendor adopting proprietary spanning tree protocols.
- To enable the digest snooping feature successfully, you must first enable it on all the ports of your device that are connected to a device of another vendor adopting proprietary spanning tree protocols and then enable it globally.
- To enable the digest snooping feature, the interconnected devices and the devices of another vendor adopting proprietary spanning tree protocols must be configured with exactly the same MST region-related configurations (including region name, revision level, and VLAN-to-MSTI mapping).
- The digest snooping feature must be enabled on all the device ports that connect to the devices of other vendors adopting proprietary spanning tree protocols in the same MST region.
- When the digest snooping feature is enabled globally, the VLAN-to-MSTI mapping table cannot be modified.
- The digest snooping feature is not applicable to boundary ports in an MST region.
- The digest snooping feature is not applicable to edge ports in an MST region.

Configuring Rapid Transition

Introduction

Designated ports of RSTP-enabled or MSTP-enabled devices use the following two types of packets to implement rapid transition:

- Proposal packets: Packets sent by designated ports to request rapid transition
- Agreement packets: Packets used to acknowledge rapid transition requests

Both RSTP and MSTP specify that the upstream device can perform rapid transition operation on the designated port only when the port receives an agreement packet from the downstream device. The difference between RSTP and MSTP are:

- For MSTP, the upstream device sends agreement packets to the downstream device; and the downstream device sends agreement packets to the upstream device only after it receives agreement packets from the upstream device.
- For RSTP, the upstream device does not send agreement packets to the downstream device.

Figure 1-6 and Figure 1-7 illustrate the rapid transition mechanisms on designated ports in RSTP and MSTP.

Figure 1-6 The RSTP rapid transition mechanism

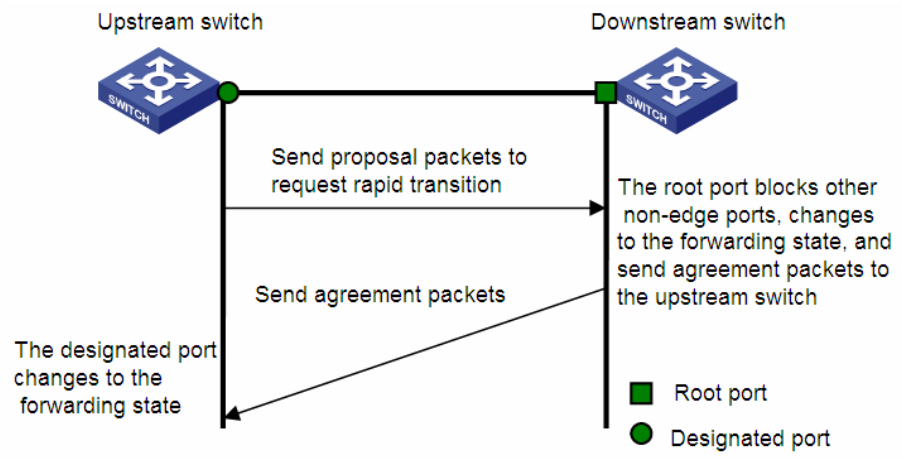
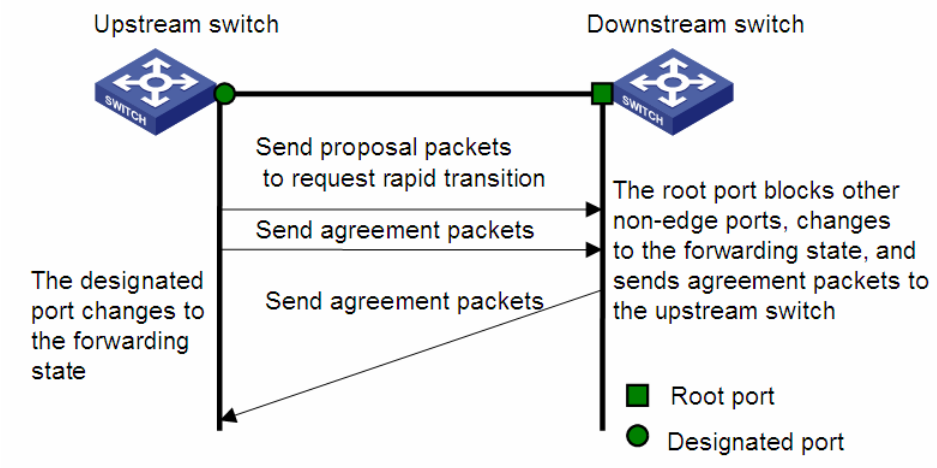


Figure 1-7 The MSTP rapid transition mechanism



The cooperation between MSTP and RSTP is limited in the process of rapid transition. For example, when the upstream device adopts RSTP, the downstream device adopts MSTP and the downstream device does not support RSTP-compatible mode, the root port on the downstream device receives no agreement packet from the upstream device and thus sends no agreement packets to the upstream device. As a result, the designated port of the upstream device fails to transit rapidly and can only turn to the forwarding state after a period twice the forward delay.

Devices of some vendors adopt proprietary spanning tree protocols that are similar to RSTP in the way to implement rapid transition on designated ports. When a device of this kind operating as the upstream device connects with a WX3000 series device running MSTP, the upstream designated port fails to change its state rapidly.

The rapid transition feature is developed to resolve this problem. When a WX3000 series device running MSTP is connected in the upstream direction to a device of another vendor running proprietary spanning tree protocols, you can enable the rapid transition feature on the ports of the WX3000 series device operating as the downstream device. Among these ports, those operating as the root ports will then send agreement packets to their upstream ports after they receive proposal packets from the upstream designated ports, instead of waiting for agreement packets from the upstream device. This enables designated ports of the upstream device to change their states rapidly.

Configuring Rapid Transition

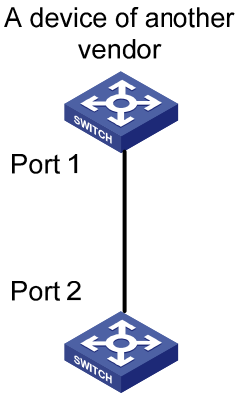
Configuration prerequisites

As shown in Figure 1-8, a WX3000 series device is connected to a device of another vendor. The former operates as the downstream device, and the latter operates as the upstream device. The network operates normally.

The upstream device is running a proprietary spanning tree protocol that is similar to RSTP in the way to implement rapid transition on designated ports. Port 1 is the designated port.

The downstream device is running MSTP. Port 2 is the root port.

Figure 1-8 Network diagram for rapid transition configuration



Configuration procedure

1) Configure the rapid transition feature in system view

Follow these steps to configure the rapid transition feature in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the rapid transition feature	**stp interface** *interface-type interface-number* **no-agreement-check**	Required By default, the rapid transition feature is disabled on a port.

2) Configure the rapid transition feature in Ethernet port view

Follow these steps to configure the rapid transition feature in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the rapid transition feature	**stp no-agreement-check**	Required By default, the rapid transition feature is disabled on a port.

Note

- The rapid transition feature can be enabled on only root ports or alternate ports.
- If you configure the rapid transition feature on a designated port, the feature does not take effect on the port.

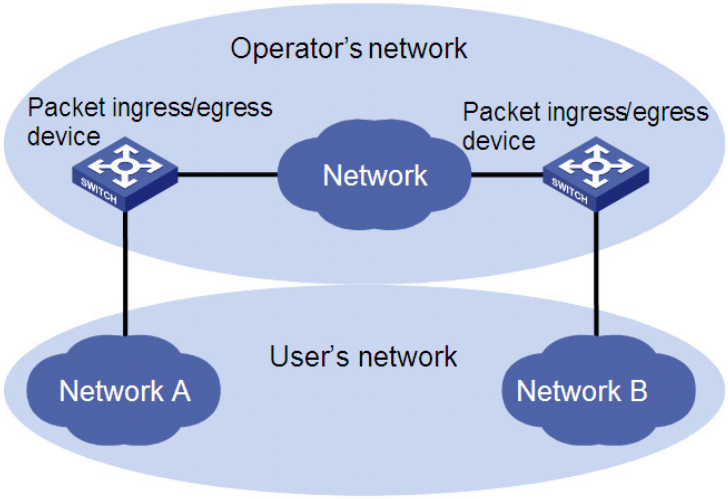
Configuring VLAN-VPN Tunnel

Introduction

The VLAN-VPN Tunnel function enables STP packets to be transparently transmitted between geographically dispersed user networks through specified VLAN VPNs in operator's networks, through which spanning trees can be generated across these user networks and are independent of those of the operator's network.

As shown in Figure 1-9, the upper part is the operator's network, and the lower part is the user's network. The operator's network comprises packet ingress/egress devices, and the user's network has networks A and B. On the operator's network, configure the arriving STP packets at the ingress to have MAC addresses in a special format, and reconvert them back to their original formats at the egress. This is how transparent transmission is implemented over the operator's network.

Figure 1-9 VLAN-VPN tunnel network hierarchy



Configuring VLAN-VPN tunnel

Follow these steps to configure VLAN-VPN tunnel:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable MSTP globally	**stp enable**	—
Enable the VLAN-VPN tunnel function globally	**vlan-vpn tunnel**	Required The VLAN-VPN tunnel function is disabled by default.

To do…	Use the command…	Remarks
Enter Ethernet port view	**interface** *interface-type interface-number*	Make sure that you enter the Ethernet port view of the port for which you want to enable the VLAN-VPN tunnel function.
Enable the VLAN VPN function for the Ethernet port	**vlan-vpn enable**	Required By default, the VLAN VPN function is disabled on all ports.

Note

- The VLAN-VPN tunnel function can be enabled on STP-enabled devices only.
- To enable the VLAN-VPN tunnel function, make sure the links between operator's networks are trunk links.

STP Maintenance Configuration

Introduction

In a large-scale network with MSTP enabled, there may be many MSTP instances, and so the status of a port may change frequently. In this case, maintenance personnel may expect that log/trap information is output to the log host when particular ports fail, so that they can check the status changes of those ports through alarm information.

Enabling Log/Trap Output for Ports of MSTP Instance

Follow these steps to enable log/trap output for ports of MSTP instance:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable log/trap output for the ports of a specified instance	**stp** [**instance** *instance-id*] **portlog**	Required By default, log/trap output is disabled for the ports of all instances.
Enable log/trap output for the ports of all instances	**stp portlog all**	Required By default, log/trap output is disabled for the ports of all instances.

Configuration Example

Enable log/trap output for the ports of instance 1.

```
<device> system-view
[device] stp instance 1 portlog
```

Enable log/trap output for the ports of all instances.

```
<device> system-view
```

```
[device] stp portlog all
```

Enabling Trap Messages Conforming to 802.1d Standard

The device sends trap messages conforming to 802.1d standard to the network management device in the following two cases:

- The device becomes the root bridge of an instance.
- Network topology changes are detected.

Configuration procedure

Follow these steps to enable trap messages conforming to 802.1d standard:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable trap messages conforming to 802.1d standard in an instance	**stp** [**instance** *instance-id*] **dot1d-trap** [**newroot** | **topologychange**] **enable**	Required

Configuration example

Enable the device to send trap messages conforming to 802.1d standard to the network management device when the device becomes the root bridge of instance 1.

```
<device> system-view
[device] stp instance 1 dot1d-trap newroot enable
```

Displaying and Maintaining MSTP

To do…	Use the command…	Remarks
Display the state and statistics information about spanning trees of the current device	**display stp** [**instance** *instance-id*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]	Available in any view
Display region configuration	**display stp region-configuration**	Available in any view
Display information about the ports that are shut down by STP protection	**display stp portdown**	Available in any view
Display information about the ports that are blocked by STP protection	**display stp abnormalport**	Available in any view
Display information about the root port of the instance where the device reside	**display stp root**	Available in any view
Clear statistics about MSTP	**reset stp** [**interface** *interface-list*]	Available in any view

MSTP Configuration Example

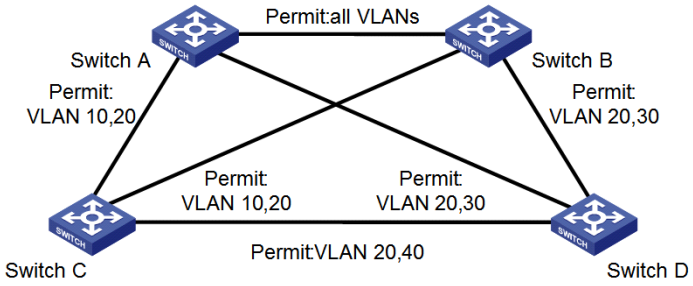
Network requirements

Implement MSTP in the network shown in Figure 1-10 to enable packets of different VLANs to be forwarded along different spanning tree instances. The detailed configurations are as follows:

- All switches in the network belong to the same MST region.
- Packets of VLAN 10, VLAN 30, VLAN 40, and VLAN 20 are forwarded along spanning tree instance 1, instance 3, instance 4, and instance 0 respectively.

In this network, Switch A and Switch B operate on the convergence layer; Switch C and Switch D operate on the access layer. VLAN 10 and VLAN 30 are limited in the convergence layer and VLAN 40 is limited in the access layer. Switch A and Switch B are configured as the root bridges of spanning tree instance 1 and spanning tree instance 3 respectively. Switch C is configured as the root bridge of spanning tree instance 4.

Figure 1-10 Network diagram for MSTP configuration



Note

The word “permit” shown in Figure 1-10 means the corresponding link permits packets of specific VLANs.

Configuration procedure

1) Configure Switch A

Enter MST region view.

```
<SwitchA> system-view
[SwitchA] stp region-configuration
```

Configure the region name, VLAN-to-MSTI mapping table, and revision level for the MST region.

```
[SwitchA-mst-region] region-name example
[SwitchA-mst-region] instance 1 vlan 10
[SwitchA-mst-region] instance 3 vlan 30
[SwitchA-mst-region] instance 4 vlan 40
[SwitchA-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[SwitchA-mst-region] active region-configuration
```

Specify Switch A as the root bridge of spanning tree instance 1.

```
[SwitchA] stp instance 1 root primary
```

2) Configure Switch B

Enter MST region view.

```
<SwitchB> system-view
[SwitchB] stp region-configuration
```

Configure the region name, VLAN-to-MSTI mapping table, and revision level for the MST region.

```
[SwitchB-mst-region] region-name example
[SwitchB-mst-region] instance 1 vlan 10
[SwitchB-mst-region] instance 3 vlan 30
[SwitchB-mst-region] instance 4 vlan 40
[SwitchB-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[SwitchB-mst-region] active region-configuration
```

Specify Switch B as the root bridge of spanning tree instance 3.

```
[SwitchB] stp instance 3 root primary
```

3) Configure Switch C.

Enter MST region view.

```
<SwitchC> system-view
[SwitchC] stp region-configuration
```

Configure the MST region.

```
[SwitchC-mst-region] region-name example
[SwitchC-mst-region] instance 1 vlan 10
[SwitchC-mst-region] instance 3 vlan 30
[SwitchC-mst-region] instance 4 vlan 40
[SwitchC-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[SwitchC-mst-region] active region-configuration
```

Specify Switch C as the root bridge of spanning tree instance 4.

```
[SwitchC] stp instance 4 root primary
```

4) Configure Switch D

Enter MST region view.

```
<SwitchD> system-view
[SwitchD] stp region-configuration
```

Configure the MST region.

```
[SwitchD-mst-region] region-name example
[SwitchD-mst-region] instance 1 vlan 10
[SwitchD-mst-region] instance 3 vlan 30
[SwitchD-mst-region] instance 4 vlan 40
[SwitchD-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[SwitchD-mst-region] active region-configuration
```

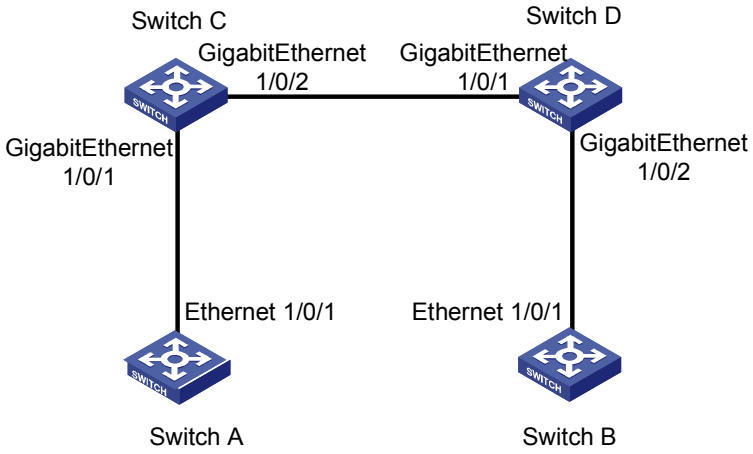
VLAN-VPN tunnel Configuration Example

Network requirements

As shown in Figure 1-11:

- The WX3000 series devices operate as the access devices of the operator's network, that is, Switch C and Switch D in the network diagram.
- Devices of other series operate as the access devices of the user's network, that is, Switch A and Switch B in the network diagram.
- Switch C and Switch D are connected to each other through the configured trunk ports of the switches. The VLAN-VPN tunnel function is enabled in system view, thus implementing transparent transmission between the user's network and the operator's network.

Figure 1-11 Network diagram for VLAN-VPN tunnel configuration



Configuration procedure

1) Configure Switch A

Enable MSTP.

```
<SwitchA> system-view
[SwitchA] stp enable
```

Add Ethernet 1/0/1 to VLAN 10.

```
[SwitchA] vlan 10
[SwitchA-Vlan10] port Ethernet1/0/1
```

2) Configure Switch B

Enable MSTP.

```
<SwitchB> system-view
[SwitchB] stp enable
```

Add Ethernet 1/0/1 to VLAN 10.

```
[SwitchB] vlan 10
[SwitchB-Vlan10] port Ethernet1/0/1
```

3) Configure Switch C

Enable MSTP.

```
<SwitchC> system-view
```

```
[SwitchC] stp enable
```

Enable the VLAN-VPN tunnel function.

```
[SwitchC] vlan-vpn tunnel
```

Add GigabitEthernet 1/0/1 to VLAN 10.

```
[SwitchC] vlan 10
[SwitchC-Vlan10] port GigabitEthernet1/0/1
[SwitchC-Vlan10] quit
```

Disable STP on GigabitEthernet 1/0/1 and then enable the VLAN VPN function on it.

```
[SwitchC] interface GigabitEthernet1/0/1
[SwitchC-GigabitEthernet1/0/1] port access vlan 10
[SwitchC-GigabitEthernet1/0/1] vlan-vpn enable
[SwitchC-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchC] interface GigabitEthernet1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
```

Add the trunk port to all VLANs.

```
[SwitchC-GigabitEthernet1/0/2] port trunk permit vlan all
```

4) Configure Switch D

Enable MSTP.

```
<SwitchD> system-view
[SwitchD] stp enable
```

Enable the VLAN-VPN tunnel function.

```
[SwitchD] vlan-vpn tunnel
```

Add GigabitEthernet 1/0/2 to VLAN 10.

```
[SwitchD] vlan 10
[SwitchD-Vlan10] port GigabitEthernet1/0/2
```

Disable STP on GigabitEthernet 1/0/2 and then enable the VLAN VPN function on it.

```
[SwitchD] interface GigabitEthernet1/0/2
[SwitchD-GigabitEthernet1/0/2] port access vlan 10
[SwitchD-GigabitEthernet1/0/2] stp disable
[SwitchD-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[SwitchD] interface GigabitEthernet1/0/1
[SwitchD-GigabitEthernet1/0/1] port link-type trunk
```

Add the trunk port to all VLANs.

```
[SwitchD-GigabitEthernet1/0/1] port trunk permit vlan all
```

Table of Contents

1 802.1x Configuration 1-1

Introduction to 802.1x 1-1

Architecture of 802.1x Authentication 1-1

The Mechanism of an 802.1x Authentication System 1-3

Encapsulation of EAPoL Messages 1-3

802.1x Authentication Procedure 1-5

Timers Used in 802.1x 1-8

Additional 802.1x Features Implemented 1-9

Introduction to 802.1x Configuration 1-11

Basic 802.1x Configuration 1-12

Configuration Prerequisites 1-12

Configuring Basic 802.1x Functions 1-12

Timer and Maximum User Number Configuration 1-14

Advanced 802.1x Configuration 1-15

Configuring Proxy Checking 1-15

Configuring Client Version Checking 1-16

Enabling DHCP-triggered Authentication 1-17

Configuring Guest VLAN 1-17

Configuring 802.1x Re-Authentication 1-18

Configuring the 802.1x Re-Authentication Timer 1-18

Displaying and Maintaining 802.1x 1-19

Configuration Example 1-19

802.1x Configuration Example 1-19

2 Quick EAD Deployment Configuration 2-1

Introduction to Quick EAD Deployment 2-1

Quick EAD Deployment Overview 2-1

Operation of Quick EAD Deployment 2-1

Configuring Quick EAD Deployment 2-1

Configuration Prerequisites 2-1

Configuration Procedure 2-2

Displaying and Maintaining Quick EAD Deployment 2-3

Quick EAD Deployment Configuration Example 2-3

Troubleshooting 2-4

3 System-Guard Configuration 3-1

System-Guard Overview 3-1

Configuring the System-Guard Feature 3-1

Configuring the System-Guard Feature 3-1

Displaying and Maintaining System-Guard 3-2

1 802.1x Configuration

Note

The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Introduction to 802.1x

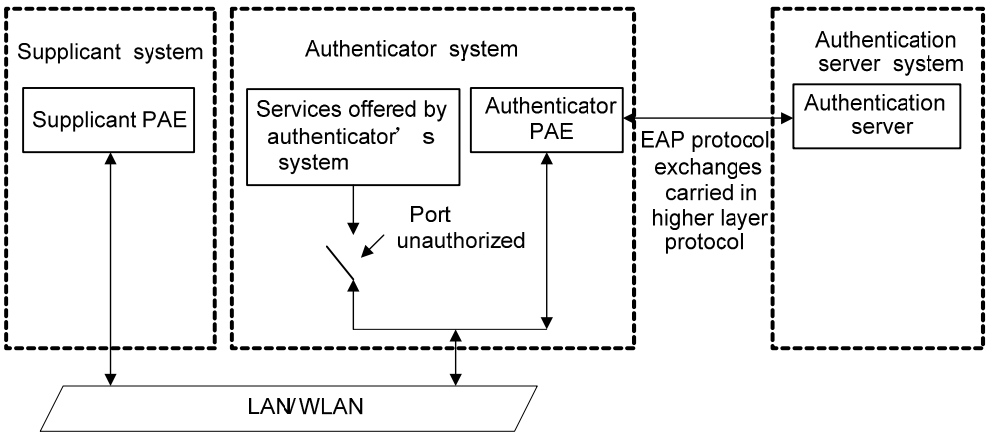
The 802.1x protocol (802.1x for short) was developed by IEEE802 LAN/WAN committee to address security issues of wireless LANs. It was then used in Ethernet as a common access control mechanism for LAN ports to address mainly authentication and security problems.

802.1x is a port-based network access control protocol. It authenticates and controls devices requesting for access in terms of the ports of LAN access devices. With the 802.1x protocol employed, a user-side device can access the LAN only when it passes the authentication. Those fail to pass the authentication are denied when accessing the LAN.

Architecture of 802.1x Authentication

As shown in Figure 1-1, 802.1x adopts a client/server architecture with three entities: a supplicant system, an authenticator system, and an authentication server system.

Figure 1-1 Architecture of 802.1x authentication



- The supplicant system is the entity seeking access the LAN. It resides at one end of a LAN segment and is authenticated by the authenticator system at the other end of the LAN segment. The supplicant system is usually a user terminal device. 802.1x authentication is triggered when a user launches an 802.1x-capable client program on the supplicant system. Note that the client program must support the extensible authentication protocol over LAN (EAPoL).

- The authenticator system, residing at the other end of the LAN segment link, is the entity that authenticates the connected supplicant system. The authenticator system is usually an 802.1x-supported network device. It provides ports (physical or logical) for the supplicant system to access the LAN.
- The authentication server system is the entity that provides authentication services to the authenticator system. The authentication server system, normally a RADIUS server, serves to perform AAA (authentication, authorization, and accounting) services to users. It also stores user information, such as user name, password, the VLAN a user should belong to, priority, and any ACLs (access control list) to be applied.

There are four additional basic concepts related to 802.1x: port access entity (PAE), controlled port and uncontrolled port, the valid direction of a controlled port and the access control method of a port.

Port access entity

A PAE (port access entity) is responsible for implementing algorithms and performing protocol-related operations in the authentication mechanism.

- The authenticator system PAE authenticates the supplicant systems when they log into the LAN and controls the status (authorized/unauthorized) of the controlled ports according to the authentication result.
- The supplicant system PAE responds to the authentication requests received from the authenticator system and submits user authentication information to the authenticator system. It also sends authentication requests and disconnection requests to the authenticator system PAE.

Controlled port and uncontrolled port

The Authenticator system provides ports for supplicant systems to access a LAN. Logically, a port of this kind is divided into a controlled port and an uncontrolled port.

- The uncontrolled port can always send and receive packets. It mainly serves to forward EAPoL packets to ensure that a supplicant system can send and receive authentication requests.
- The controlled port can be used to pass service packets when it is in authorized state. It is blocked when not in authorized state. In this case, no packets can pass through it.
- Controlled port and uncontrolled port are two properties of a port. Packets reaching a port are visible to both the controlled port and uncontrolled port of the port.

The valid direction of a controlled port

When a controlled port is in unauthorized state, you can configure it to be a unidirectional port, which only sends packets out to supplicant systems.

By default, a controlled port is a unidirectional port.

Port access control method

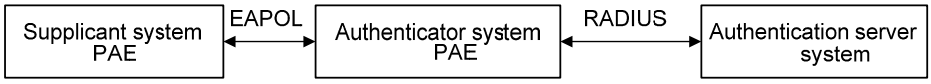
A port of the device can control user accesses in the following two ways.

- Port-based control. When a port works in the port-based control mode, all the supplicant systems connected to the port can access the network without being authenticated after one supplicant system among them passes the authentication. And when the authenticated supplicant system goes offline, the others are denied as well.
- MAC-based control. When a port works in the MAC-based control mode, all supplicant systems connected to the port have to be authenticated individually in order to access the network. And when a supplicant system goes offline, the others are not affected.

The Mechanism of an 802.1x Authentication System

IEEE 802.1x authentication uses the extensible authentication protocol (EAP) to exchange information between supplicant systems and the authentication servers. To be compatible with 802.1X in a LAN environment, the client program must support the Extensible Authentication Protocol over LAN (EAPoL).

Figure 1-2 The mechanism of an 802.1x authentication system



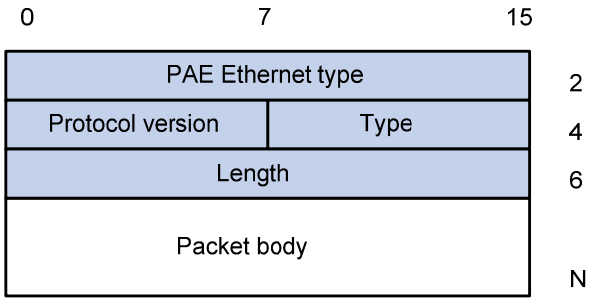
- EAP protocol packets transmitted between the supplicant system PAE and the authenticator system PAE are encapsulated as EAPoL packets.
- EAP protocol packets transmitted between the authenticator system PAE and the RADIUS server can either be encapsulated as EAP over RADIUS (EAPoR) packets or be terminated at system PAEs. The system PAEs then communicate with RADIUS servers through password authentication protocol (PAP) or challenge-handshake authentication protocol (CHAP) packets.
- When a supplicant system passes the authentication, the authentication server passes the information about the supplicant system to the authenticator system. The authenticator system in turn determines the state (authorized or unauthorized) of the controlled port according to the instructions (accept or reject) received from the RADIUS server.

Encapsulation of EAPoL Messages

The format of an EAPoL packet

EAPoL is a packet encapsulation format defined in 802.1x. To enable EAP protocol packets to be transmitted between supplicant systems and authenticator systems through LANs, EAP protocol packets are encapsulated in EAPoL format. The following figure illustrates the structure of an EAPoL packet.

Figure 1-3 The format of an EAPoL packet



In an EAPoL packet:

- The PAE Ethernet type field holds the protocol identifier. The identifier for 802.1x is 0x888E.
- The Protocol version field holds the version of the protocol supported by the sender of the EAPoL packet.
- The Type field can be one of the following:
  00: Indicates that the packet is an EAP-packet, which carries authentication information.
  01: Indicates that the packet is an EAPoL-start packet, which initiates the authentication.
  02: Indicates that the packet is an EAPoL-logoff packet, which sends logging off requests.

03: Indicates that the packet is an EAPoL-key packet, which carries key information.

04: Indicates that the packet is an EAPoL-encapsulated-ASF-Alert packet, which is used to support the alerting messages of ASF (alerting standards forum).

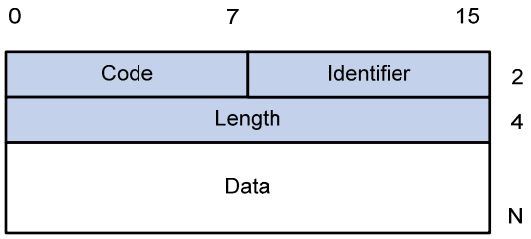
- The Length field indicates the size of the Packet body field. A value of 0 indicates that the Packet Body field does not exist.
- The Packet body field differs with the Type field.

Note that EAPoL-Start, EAPoL-Logoff, and EAPoL-Key packets are only transmitted between the supplicant system and the authenticator system. EAP-packets are encapsulated by RADIUS protocol to allow them successfully reach the authentication servers. Network management-related information (such as alarming information) is encapsulated in EAPoL-Encapsulated-ASF-Alert packets, which are terminated by authenticator systems.

The format of an EAP packet

For an EAPoL packet with the value of the Type field being EAP-packet, its Packet body field is an EAP packet, whose format is illustrated in Figure 1-4.

Figure 1-4 The format of an EAP packet



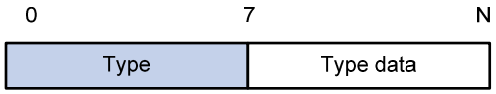
In an EAP packet:

- The Code field indicates the EAP packet type, which can be Request, Response, Success, or Failure.
- The Identifier field is used to match a Response packet with the corresponding Request packet.
- The Length field indicates the size of an EAP packet, which includes the Code, Identifier, Length, and Data fields.
- The Data field carries the EAP packet, whose format differs with the Code field.

A Success or Failure packet does not contain the Data field, so the Length field of it is 4.

Figure 1-5 shows the format of the Data field of a Request packet or a Response packet.

Figure 1-5 The format of the Data field of a Request packet or a Response packet



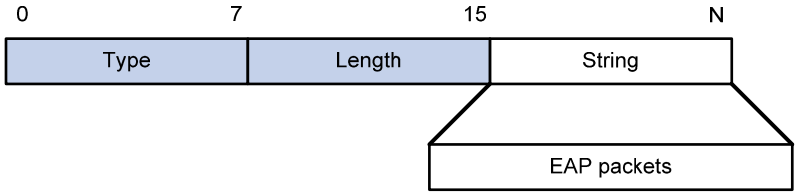
- The Type field indicates the EAP authentication type. A value of 1 indicates Identity and that the packet is used to query the identity of the peer. A value of 4 represents MD5-Challenge (similar to PPP CHAP) and indicates that the packet includes query information.
- The Type Date field differs with types of Request and Response packets.

Fields added for EAP authentication

Two fields, EAP-message and Message-authenticator, are added to a RADIUS protocol packet for EAP authentication. (Refer to the Introduction to RADIUS protocol section in the *AAA Operation Manual* for information about the format of a RADIUS protocol packet.)

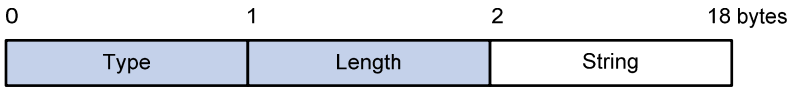
The EAP-message field, whose format is shown in Figure 1-6, is used to encapsulate EAP packets. The maximum size of the string field is 253 bytes. EAP packets with their size larger than 253 bytes are fragmented and are encapsulated in multiple EAP-message fields. The type code of the EAP-message field is 79.

Figure 1-6 The format of an EAP-message field



The Message-authenticator field, whose format is shown in Figure 1-7, is used to prevent unauthorized interception to access requesting packets during authentications using CHAP, EAP, and so on. A packet with the EAP-message field must also have the Message-authenticator field. Otherwise, the packet is regarded as invalid and is discarded.

Figure 1-7 The format of an Message-authenticator field



802.1x Authentication Procedure

The device can authenticate supplicant systems in EAP terminating mode or EAP relay mode.

EAP relay mode

This mode is defined in 802.1x. In this mode, EAP-packets are encapsulated in higher level protocol (such as EAPoR) packets to enable them to successfully reach the authentication server. Normally, this mode requires that the RADIUS server support the two newly-added fields: the EAP-message field (with a value of 79) and the Message-authenticator field (with a value of 80).

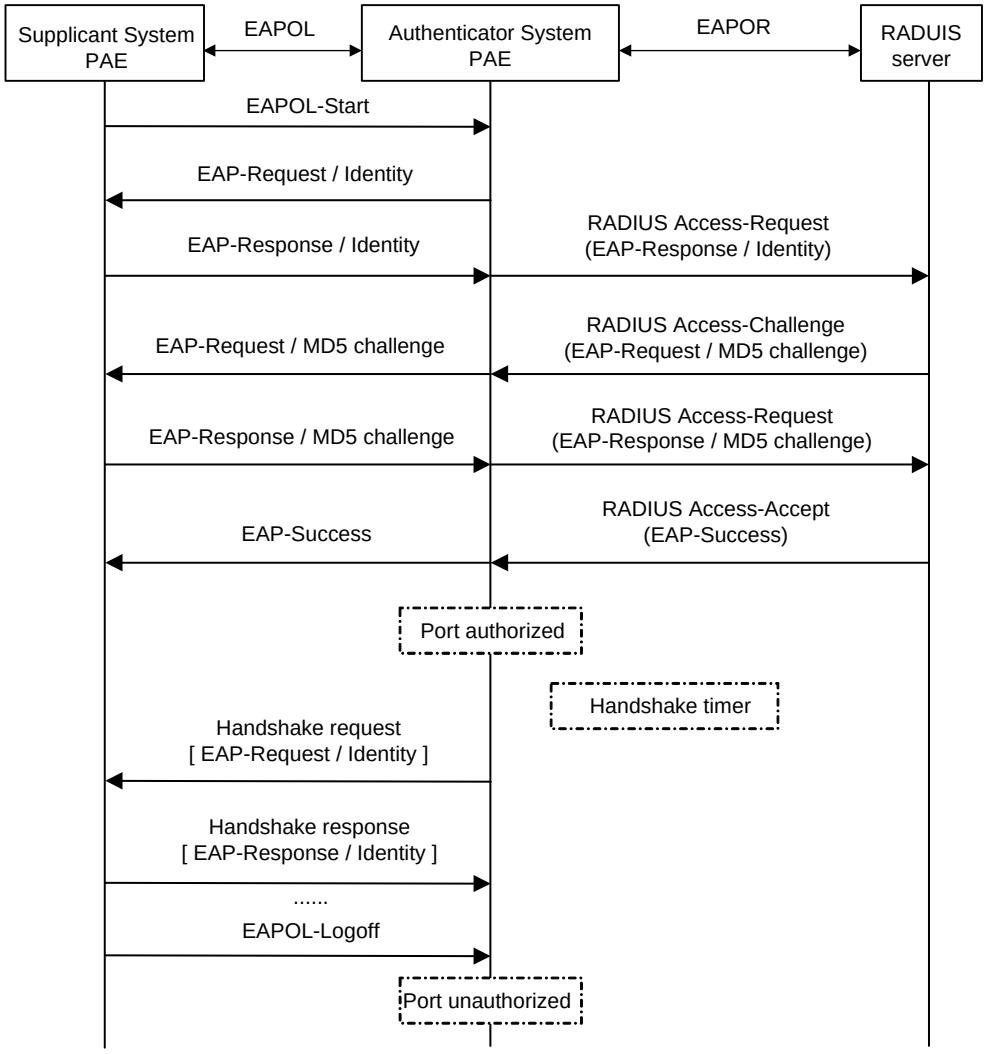
Four authentication ways, namely EAP-MD5, EAP-TLS (transport layer security), EAP-TTLS (tunneled transport layer security), and PEAP (protected extensible authentication protocol), are available in the EAP relay mode.

- EAP-MD5 authenticates the supplicant system. The RADIUS server sends MD5 keys (contained in EAP-request/MD5 challenge packets) to the supplicant system, which in turn encrypts the passwords using the MD5 keys.
- EAP-TLS allows the supplicant system and the RADIUS server to check each other's security certificate and authenticate each other's identity, guaranteeing that data is transferred to the right destination and preventing data from being intercepted.

- EAP-TTLS is a kind of extended EAP-TLS. EAP-TLS implements bidirectional authentication between the client and authentication server. EAP-TTLS transmit message using a tunnel established using TLS.
- PEAP creates and uses TLS security channels to ensure data integrity and then performs new EAP negotiations to verify supplicant systems.

Figure 1-8 describes the basic EAP-MD5 authentication procedure.

Figure 1-8 802.1x authentication procedure (in EAP relay mode)



The detailed procedure is as follows:

- A supplicant launches an iNode client, and then provides the valid user name and password on the iNode client to initiate a connection request. In this case, the iNode client program sends the connection request (the EAPoL-start packet) to the device to start the authentication process.
- Upon receiving the authentication request packet, the device sends an EAP-request/identity packet to ask the iNode client for the user name.
- The iNode client responds by sending an EAP-response/identity packet to the device with the user name contained in it. The device then encapsulates the packet in a RADIUS Access-Request packet and forwards it to the RADIUS server.
- Upon receiving the packet from the device, the RADIUS server retrieves the user name from the packet, finds the corresponding password by matching the user name in its database, encrypts the

password using a randomly-generated key, and sends the key to the device through an RADIUS access-challenge packet. The device then sends the key to the iNode client.

- Upon receiving the key (encapsulated in an EAP-request/MD5 challenge packet) from the device, the client program encrypts the password of the supplicant system with the key and sends the encrypted password (contained in an EAP-response/MD5 challenge packet) to the RADIUS server through the device. (Normally, the encryption is irreversible.)
- The RADIUS server compares the received encrypted password (contained in a RADIUS access-request packet) with the locally-encrypted password. If the two match, it will then send feedbacks (through a RADIUS access-accept packet and an EAP-success packet) to the device to indicate that the supplicant is authenticated.
- The device changes the state of the corresponding port to accepted state to allow the supplicant to access the network.
- The supplicant can also terminate the authenticated state by sending EAPoL-Logoff packets to the device. The device then changes the port state from accepted to rejected.

Note

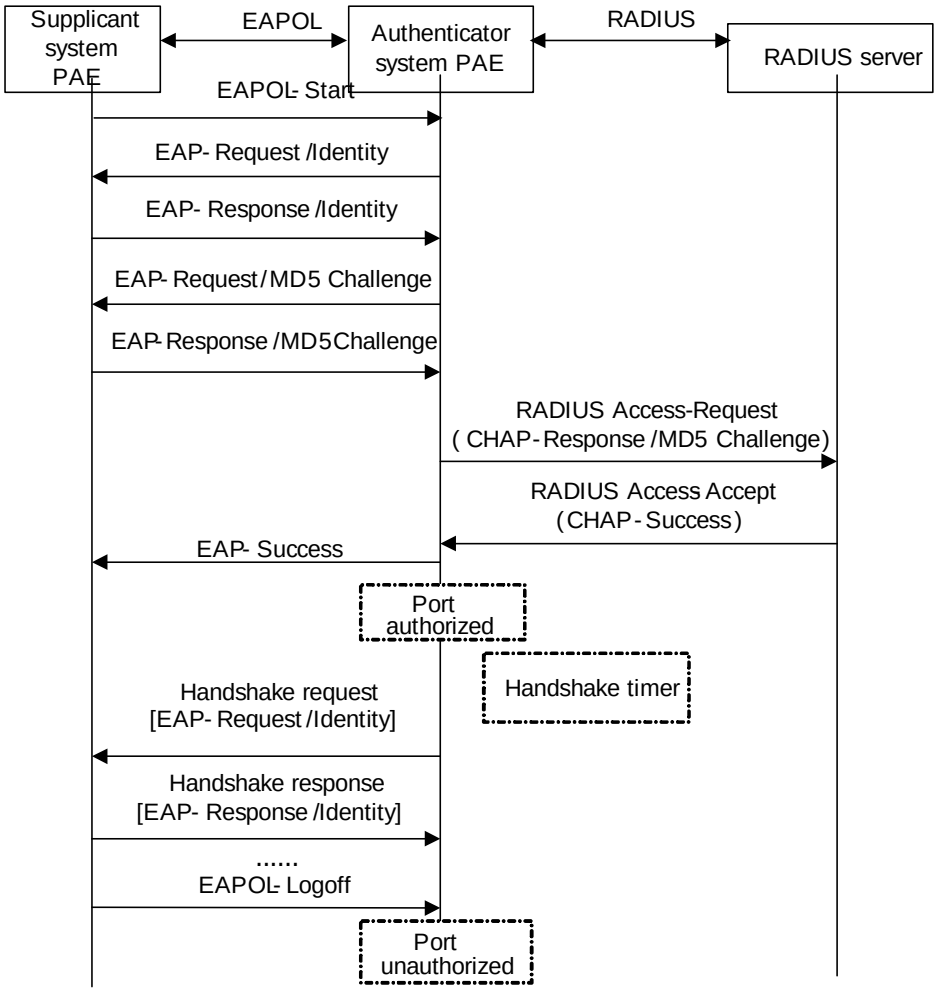
When you configure your device to work in EAP relay mode, you do not need to configure the authentication method to be used. The device and the RADIUS server will negotiate one. The negotiation is initiated by the RADIUS server. Different RADIUS servers support different authentication methods and the order of PEAP, EAP-TLS, EAP-TTLS, and EAP-MD5 in the negotiation may vary.

EAP terminating mode

In this mode, EAP packet transmission is terminated at authenticator systems and the EAP packets are converted to RADIUS packets. Authentication and accounting are carried out through RADIUS protocol.

In this mode, PAP or CHAP is employed between the device and the RADIUS server. Figure 1-9 illustrates the authentication procedure (assuming that CHAP is employed between the device and the RADIUS server).

Figure 1-9 802.1x authentication procedure (in EAP terminating mode)



The authentication procedure in EAP terminating mode is the same as that in the EAP relay mode except that the randomly-generated key in the EAP terminating mode is generated by the device, and that it is the device that sends the user name, the randomly-generated key, and the supplicant system-encrypted password to the RADIUS server for further authentication.

Timers Used in 802.1x

In 802.1 x authentication, the following timers are used to ensure that the supplicant system, the device, and the RADIUS server interact in an orderly way.

- Handshake timer (**handshake-period**). This timer sets the handshake-period and is triggered after a supplicant system passes the authentication. It sets the interval for the device to send handshake request packets to online users. You can set the number of retries by using the **dot1x retry** command. An online user will be considered offline when the device has not received any response packets after a certain number of handshake request transmission retries.
- Quiet-period timer (**quiet-period**). This timer sets the quiet-period. When a supplicant system fails to pass the authentication, the device quiets for the set period (set by the quiet-period timer) before it processes another authentication request re-initiated by the supplicant system. During this quiet period, the device does not perform any 802.1x authentication-related actions for the supplicant system.
- Re-authentication timer (**reauth-period**). The device will initiate 802.1x re-authentication at the interval set by the re-authentication timer.

- RADIUS server timer (**server-timeout**). This timer sets the server-timeout period. After sending an authentication request packet to the RADIUS server, the device sends another authentication request packet if it does not receive the response from the RADIUS server when this timer times out.
- Supplicant system timer (**supp-timeout**). This timer sets the supp-timeout period and is triggered by the device after the device sends a request/challenge packet to a supplicant system. The device sends another request/challenge packet to the supplicant system if the device does not receive the response from the supplicant system when this timer times out.
- Transmission timer (**tx-period**). This timer sets the tx-period and is triggered by the device in two cases. The first case is when the client requests for authentication. The device sends a unicast request/identity packet to a supplicant system and then triggers the transmission timer. The device sends another request/identity packet to the supplicant system if it does not receive the reply packet from the supplicant system when this timer times out. The second case is when the device authenticates the iNode client who cannot request for authentication actively. The device sends multicast request/identity packets periodically through the port enabled with 802.1x function. In this case, this timer sets the interval to send the multicast request/identity packets.
- Client version request timer (**ver-period**). This timer sets the version period and is triggered after the device sends a version request packet. The device sends another version request packet if it does receive version response packets from the supplicant system when the timer expires.

Additional 802.1x Features Implemented

In addition to the earlier mentioned 802.1x features, the device is also capable of the following:

- Checking supplicant systems for proxies, multiple network adapters, etc (This function needs the cooperation of a iMC server.)
- Checking client version
- The Guest VLAN function

Note

iMC Server is a service management system used to manage networks and to secure networks and user information. With the cooperation of other networking devices (such as the WX3000 series devices) in the network, a iMC server can implement the AAA functions and rights management.

Checking the supplicant system

The device checks:

- Supplicant systems logging on through proxies
- Supplicant systems logging on through IE proxies
- Whether or not a supplicant system logs in through more than one network adapters (that is, whether or not more than one network adapters are active in a supplicant system when the supplicant system logs in).

In response to any of the three cases, the device can optionally take the following measures:

- Only disconnects the supplicant system but sends no Trap packets.
- Sends Trap packets without disconnecting the supplicant system.

This function needs the cooperation of iNode client and a iMC server.

- The iNode client needs to capable of detecting multiple network adapters, proxies, and IE proxies.
- The iMC server is configured to disable the use of multiple network adapters, proxies, or IE proxies.

By default, an iNode client program allows use of multiple network adapters, proxies, and IE proxies. In this case, if the iMC server is configured to disable use of multiple network adapters, proxies, or IE proxies, it prompts the iNode client to disable use of multiple network adapters, proxies, or IE proxies through messages after the supplicant system passes the authentication.

 **Note**

- The client-checking function needs the support of iNode client program.
- To implement the proxy detecting function, you need to enable the function on both the iNode client program and the iMC server in addition to enabling the client version checking function on the device by using the **dot1x version-check** command.

Checking the client version

With the iNode client version-checking function enabled, the device checks the version and validity of an iNode client to prevent unauthorized users or users with earlier versions of iNode client from logging in.

This function makes the device to send version-requesting packets again if the iNode client fails to send version-reply packet to the device when the version-checking timer times out.

 **Note**

The iNode client version-checking function needs the support of an iNode client program.

The Guest VLAN function

The Guest VLAN function enables supplicant systems that are not authenticated to access network resources in a restrained way.

The Guest VLAN function enables supplicant systems that do not have iNode client installed to access specific network resources. It also enables supplicant systems that are not authenticated to upgrade their iNode client programs.

With this function enabled:

- The device sends authentication request (EAP-Request/Identity) packets to all the 802.1x-enabled ports.
- After the maximum number retries have been made and there are still ports that have not sent any response back, the device will then add these ports to the Guest VLAN.
- Users belonging to the Guest VLAN can access the resources of the Guest VLAN without being authenticated. But they need to be authenticated when accessing external resources.

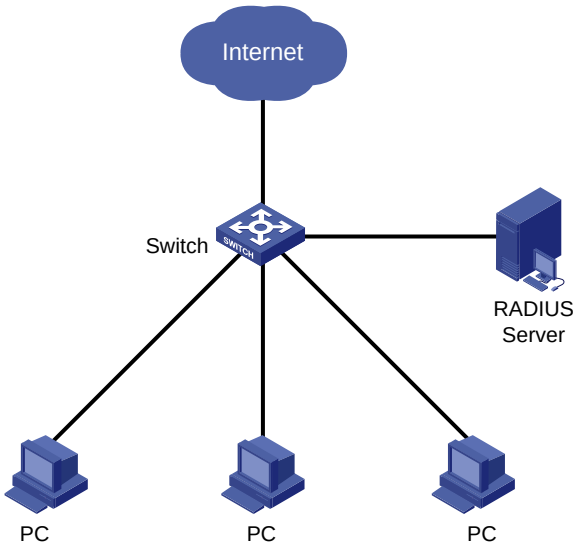
Normally, the Guest VLAN function is coupled with the dynamic VLAN delivery function.

Refer to *AAA Operation Manual* for detailed information about the dynamic VLAN delivery function.

Enabling 802.1x re-authentication

802.1x re-authentication is timer-triggered or packet-triggered. It re-authenticates users who have passed authentication. With 802.1x re-authentication enabled, the device can monitor the connection status of users periodically. If the device receives no re-authentication response from a user in a period of time, it tears down the connection to the user. To connect to the device again, the user needs to initiate 802.1x authentication with the client software again.

Figure 1-10 802.1x re-authentication



802.1x re-authentication can be enabled in one of the following two ways:

- The RADIUS server triggers the device to perform 802.1x re-authentication of users. The RADIUS server sends the device an Access-Accept packet with the Termination-Action attribute field of 1. Upon receiving the packet, the device re-authenticates users periodically.
- You enable 802.1x re-authentication on the device. With 802.1x re-authentication enabled, the device re-authenticates users periodically.

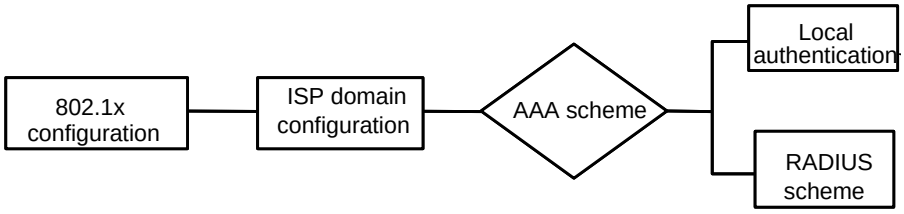
Note

802.1x re-authentication will fail if a iMC server is used and configured to perform authentication but not accounting. This is because a iMC server establishes a user session after it begins to perform accounting. Therefore, to enable 802.1x re-authentication, do not configure the **accounting none** command in the domain. This restriction does not apply to other types of servers.

Introduction to 802.1x Configuration

802.1x provides a solution for authenticating users. To implement this solution, you need to execute 802.1x-related commands. You also need to configure AAA schemes on the device and specify the authentication scheme (RADIUS, HWTACACS or local authentication scheme).

Figure 1-11 802.1x configuration



- An 802.1x user uses the domain name to associate with the ISP domain configured on the device.
- Configure the AAA scheme (a local authentication scheme, a RADIUS scheme or a HWTACACS scheme) to be adopted in the ISP domain.
- If you specify to use a local authentication scheme, you need to configure the user names and passwords manually on the device. Users can pass the authentication through iNode client if they provide user names and passwords that match those configured on the device.
- If you specify to adopt the RADIUS scheme, users are authenticated by a remote RADIUS server. In this case, you need to configure user names and passwords on the RADIUS server and perform RADIUS client-related configuration on the device.
- If you specify to adopt the HWTACACS scheme, users are authenticated by a remote TACACS server. In this case, you need to configure user names and passwords on the TACACS server and perform HWTACACS client-related configuration on the device.
- You can also specify to adopt the RADIUS or HWTACACS authentication scheme, with a local authentication scheme as a backup. In this case, the local authentication scheme is adopted when the RADIUS server or the TACACS server fails.

Refer to the *AAA Operation Manual* for detailed information about AAA scheme configuration.

Basic 802.1x Configuration

Configuration Prerequisites

- Configure ISP domain and the AAA scheme to be adopted. You can specify a RADIUS scheme, a HWTACACS scheme, or a local scheme.
- Ensure that the service type is configured as **lan-access** (by using the **service-type** command) if local authentication scheme is adopted.

Configuring Basic 802.1x Functions

Follow these steps to configure basic 802.1x functions:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable 802.1x globally	**dot1x**	Required By default, 802.1x is disabled globally.

To do…		Use the command…	Remarks
Enable 802.1x for specified ports	In system view	**dot1x** [**interface** *interface-list*]	Required By default, 802.1x is disabled on all ports.
	In port view	**interface** *interface-type interface-number*	
		dot1x	
		quit	
Set port authorization mode for specified ports		**dot1x port-control** { **authorized-force** | **unauthorized-force** | **auto** } [**interface** *interface-list*]	Optional By default, an 802.1x-enabled port operates in the **auto** mode.
Set the access control method for specified ports		**dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]	Optional The default access control method on a port is MAC-based (that is, the **macbased** keyword is used by default).
Set authentication method for 802.1x users		**dot1x authentication-method** { **chap** | **pap** | **eap** }	Optional By default, the device performs CHAP authentication in EAP terminating mode.
Enable online user handshaking		**dot1x handshake enable**	Optional By default, online user handshaking is enabled.
Enter Ethernet port view		**interface** *interface-type interface-number*	—
Enable the handshaking packet secure function		**dot1x handshake secure**	Optional By default, the handshaking secure function is disabled.

Caution

- 802.1x configurations take effect only after you enable 802.1x both globally and for specified ports.
- If you enable 802.1x for a port, you cannot set the maximum number of MAC addresses that can be learnt for the port. Meanwhile, if you set the maximum number of MAC addresses that can be learnt for a port, it is prohibited to enable 802.1x for the port.
- If you enable 802.1x for a port, it is not available to add the port to an aggregation group. Meanwhile, if a port has been added to an aggregation group, it is prohibited to enable 802.1x for the port.
- Changing the access control method on a port by the **dot1x port-method** command will forcibly log out the online 802.1x users on the port.
- When the device itself operates as an authentication server, its authentication method for 802.1x users cannot be configured as EAP.
- Handshaking packets are used to test whether a user is online or not. Users need to run the proprietary iNode client software to respond to the handshaking packets.
- As clients not running the iNode client software do not support the online user handshaking function, the device cannot receive handshaking acknowledgement packets from the client in handshaking periods. To prevent the user being falsely considered offline, you need to disable the online user handshaking function in this case.
- For the handshaking packet secure function to take effect, the clients that enable the function need to cooperate with the authentication server. If either the clients or the authentication server does not support the function, disabling the handshaking packet secure function is needed.

Timer and Maximum User Number Configuration

Follow these steps to configure 802.1x timers and the maximum number of users:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Set the maximum number of concurrent on-line users for specified ports	In system view	**dot1x max-user** *user-number* [**interface** *interface-list*]	Optional By default, a port can accommodate up to 256 users at a time.
	In port view	**interface** *interface-type interface-number*	
		dot1x max-user *user-number*	
		quit	
Set the maximum retry times to send request packets		**dot1x retry** *max-retry-value*	Optional By default, the maximum retry times to send a request packet is 2. That is, the authenticator system sends a request packet to a supplicant system for up to two times by default.

To do…	Use the command…	Remarks
Set 802.1x timers	**dot1x timer** { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* | **ver-period** *ver-period-value* }	Optional The settings of 802.1x timers are as follows. • *handshake-period-value:* 15 seconds • *quiet-period-value:* 60 seconds • *server-timeout-value:* 100 seconds • *supp-timeout-value:* 30 seconds • *tx-period-value:* 30 seconds • *ver-period-value:* 30 seconds
Enable the quiet-period timer	**dot1x quiet-period**	Optional By default, the quiet-period timer is disabled.

Note

- As for the **dot1x max-user** command, if you execute it in system view without specifying the *interface-list* argument, the command applies to all ports. You can also use this command in port view. In this case, this command applies to the current port only and the *interface-list* argument is not needed.
- As for the configuration of 802.1x timers, the default values are recommended.

Advanced 802.1x Configuration

Advanced 802.1x configurations, as listed below, are all optional.

- Configuration concerning iMC, including multiple network adapters detecting, proxy detecting, and so on.
- Client version checking configuration
- DHCP–triggered authentication
- Guest VLAN configuration
- 802.1x re-authentication configuration
- Configuration of the 802.1x re-authentication timer

You need to configure basic 802.1x functions before configuring the above 802.1x features.

Configuring Proxy Checking

Follow these steps to configure proxy checking:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable proxy checking function globally	**dot1x supp-proxy-check** { **logoff** | **trap** }	Required By default, the 802.1x proxy checking function is globally disabled.

To do…		Use the command…	Remarks
Enable proxy checking for a port/specified ports	In system view	**dot1x supp-proxy-check** { **logoff** | **trap** } [**interface** *interface-list*]	Required By default, the 802.1x proxy checking is disabled on a port.
	In port view	**interface** *interface-type interface-number*	
		dot1x supp-proxy-check { **logoff** | **trap** }	
		quit	

Note

- The proxy checking function needs the cooperation of an iNode client program.
- The proxy checking function depends on the online user handshaking function. To enable the proxy detecting function, you need to enable the online user handshaking function first.
- The configuration listed in the table above takes effect only when it is performed on iMC as well as on the device. In addition, the client version checking function needs to be enabled on the device too (by using the **dot1x version-check** command).

Configuring Client Version Checking

Follow these steps to configure client version checking:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enable iNode client version checking	In system view	**dot1x version-check** [**interface** *interface-list*]	Required By default, iNode client version checking is disabled on a port.
	In port view	**interface** *interface-type interface-number*	
		dot1x version-check	
		quit	
Set the maximum number of retires to send version checking request packets		**dot1x retry-version-max** *max-retry-version-value*	Optional By default, the maximum number of retires to send version checking request packets is 3.
Set the client version checking period timer		**dot1x timer ver-period** *ver-period-value*	Optional By default, the timer is set to 30 seconds.

Note

As for the **dot1x version-user** command, if you execute it in system view without specifying the *interface-list* argument, the command applies to all ports. You can also execute this command in port view. In this case, this command applies to the current port only and the *interface-list* argument is not needed.

Enabling DHCP-triggered Authentication

After performing the following configuration, 802.1x allows running DHCP on access users, and users are authenticated when they apply for dynamic IP addresses through DHCP.

Follow these steps to enable DHCP-triggered authentication:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable DHCP-triggered authentication	**dot1x dhcp-launch**	Required By default, DHCP-triggered authentication is disabled.

Configuring Guest VLAN

Follow these steps to configure Guest VLAN:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the access control method on ports	**dot1x port-method portbased**	Required The default access control method on ports is MAC-based. That is, the **macbased** keyword is used by default.
Enable the Guest VLAN function	**dot1x guest-vlan** *vlan-id* [**interface** *interface-list*]	Required By default, the Guest VLAN function is disabled.

Caution

- The Guest VLAN function is available only when the device operates in the port-based access control mode.
- Only one Guest VLAN can be configured for each device.
- The Guest VLAN function cannot be implemented if you configure the **dot1x dhcp-launch** command on the device to enable DHCP-triggered authentication. This is because the device does not send authentication packets unsolicitedly in that case.

Configuring 802.1x Re-Authentication

Follow these steps to enable 802.1x re-authentication:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enable 802.1x globally		**dot1x**	Required By default, 802.1x is disabled globally.
Enable 802.1x for specified ports	In system view	**dot1x** [**interface** *interface-list*]	Required By default, 802.1x is disabled on all ports.
	In port view	**dot1x**	
Enable 802.1x re-authentication on port(s)	In system view	**dot1x re-authenticate** [**interface** *interface-list*]	Required By default, 802.1x re-authentication is disabled on a port.
	In port view	**dot1x re-authenticate**	

Note

To enable 802.1x re-authentication on a port, you must first enable 802.1x globally and on the port.

Configuring the 802.1x Re-Authentication Timer

After 802.1x re-authentication is enabled on the device, the device determines the re-authentication interval in one of the following two ways:

1) The device uses the value of the Session-timeout attribute field of the Access-Accept packet sent by the RADIUS server as the re-authentication interval.
2) The device uses the value configured with the **dot1x timer reauth-period** command as the re-authentication interval for access users.

Note the following:

During re-authentication, the device always uses the latest re-authentication interval configured, no matter which of the above-mentioned two ways is used to determine the re-authentication interval. For example, if you configure a re-authentication interval on the device and the device receives an Access-Accept packet whose Termination-Action attribute field is 1, the device will ultimately use the value of the Session-timeout attribute field as the re-authentication interval.

The following introduces how to configure the 802.1x re-authentication timer on the device.

Follow these steps to configure the re-authentication interval:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a re-authentication interval	**dot1x timer reauth-period** *reauth-period-value*	Optional By default, the re-authentication interval is 3,600 seconds.

Displaying and Maintaining 802.1x

To do…	Use the command…	Remarks
Display the configuration, session, and statistics information about 802.1x	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]	Available in any view.
Clear 802.1x-related statistics information	**reset dot1x statistics** [**interface** *interface-list*]	Available in user view.

Configuration Example

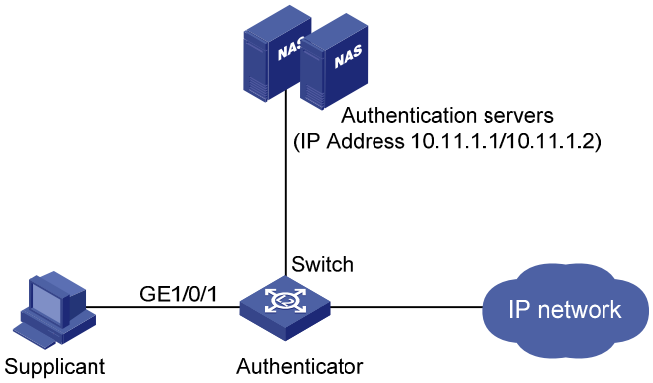
802.1x Configuration Example

Network requirements

As shown in Figure 1-12:

- Authenticate users on all ports to control their accesses to the Internet. The device (Switch) operates in MAC-based access control mode.
- All supplicant systems that pass the authentication belong to the default domain named “aabbcc.net”. The domain can accommodate up to 30 users. As for authentication, a supplicant system is authenticated locally if the RADIUS server fails. And as for accounting, a supplicant system is disconnected by force if the RADIUS server fails. The name of an authenticated supplicant system is not suffixed with the domain name. A connection is terminated if the total size of the data passes through it during a period of 20 minutes is less than 2,000 bytes.
- The device is connected to a server comprising of two RADIUS servers whose IP addresses are 10.11.1.1 and 10.11.1.2. The RADIUS server with an IP address of 10.11.1.1 operates as the primary authentication server and the secondary accounting server. The other operates as the secondary authentication server and primary accounting server. The password for the device and the authentication RADIUS servers to exchange message is “name”. And the password for the device and the accounting RADIUS servers to exchange message is “money”. The device sends another packet to the RADIUS servers again if it sends a packet to the RADIUS server and does not receive response for 5 seconds, with the maximum number of retries of 5. And the device sends a real-time accounting packet to the RADIUS servers once in every 15 minutes. A user name is sent to the RADIUS servers with the domain name truncated.
- The user name and password for local 802.1x authentication are “localuser” and “localpass” (in plain text) respectively. The idle disconnecting function is enabled.

Figure 1-12 Network diagram for AAA configuration with 802.1x and RADIUS enabled



Configuration procedure

Note

Following configuration covers the major AAA/RADIUS configuration commands. Refer to *AAA Operation Manual* for the information about these commands. Configuration on the client and the RADIUS servers is omitted.

Enable 802.1x globally.

```
<device> system-view
System View: return to User View with Ctrl+Z.
[device] dot1x
```

Enable 802.1x on GigabitEthernet 1/0/1 port.

```
[device] dot1x interface GigabitEthernet 1/0/1
```

Set the access control method to be MAC-address-based (This operation can be omitted, as MAC-address-based is the default).

```
[device] dot1x port-method macbased interface GigabitEthernet 1/0/1
```

Create a RADIUS scheme named “radius1” and enter RADIUS scheme view.

```
[device] radius scheme radius1
```

Assign IP addresses to the primary authentication and accounting RADIUS servers.

```
[device-radius-radius1] primary authentication 10.11.1.1
[device-radius-radius1] primary accounting 10.11.1.2
```

Assign IP addresses to the secondary authentication and accounting RADIUS server.

```
[device-radius-radius1] secondary authentication 10.11.1.2
[device-radius-radius1] secondary accounting 10.11.1.1
```

Set the password for the switch and the authentication RADIUS servers to exchange messages.

```
[device-radius-radius1] key authentication name
```

Set the password for the switch and the accounting RADIUS servers to exchange messages.

```
[device-radius-radius1] key accounting money
```

Set the interval and the number of the retries for the switch to send packets to the RADIUS servers.

```
[device-radius-radius1] timer 5
[device-radius-radius1] retry 5
```

Set the timer for the switch to send real-time accounting packets to the RADIUS servers.

```
[device-radius-radius1] timer realtime-accounting 15
```

Configure to send the user name to the RADIUS server with the domain name truncated.

```
[device-radius-radius1] user-name-format without-domain
[device-radius-radius1] quit
```

Create the domain named “aabbcc.net” and enter its view.

```
[device] domain enable aabbcc.net
```

Specify to adopt radius1 as the RADIUS scheme of the user domain. If RADIUS server is invalid, specify to adopt the local authentication scheme.

```
[device-isp-aabbcc.net] scheme radius-scheme radius1 local
```

Specify the maximum number of users the user domain can accommodate to 30.

```
[device-isp-aabbcc.net] access-limit enable 30
```

Enable the idle disconnecting function and set the related parameters.

```
[device-isp-aabbcc.net] idle-cut enable 20 2000
[device-isp-aabbcc.net] quit
```

Set the default user domain to be “aabbcc.net”.

```
[device] domain default enable aabbcc.net
```

Create a local access user account.

```
[device] local-user localuser
[device-luser-localuser] service-type lan-access
[device-luser-localuser] password simple localpass
```

2 Quick EAD Deployment Configuration

Introduction to Quick EAD Deployment

Quick EAD Deployment Overview

As an integrated solution, an endpoint admission defense (EAD) solution can improve the overall defense power of a network. In real applications, however, deploying EAD clients proves to be time-consuming and inconvenient.

The device enables the quick deployment of EAD clients by implementing mandatory EAD client distribution through 802.1x authentication.

Operation of Quick EAD Deployment

The device implements quick EAD deployment by leveraging the following two functions to enable mandatory EAD client distribution:

Restricted access

Before passing 802.1x authentication, a user is restricted (through ACLs) to a specific range of IP addresses or a specific server. Services like EAD client upgrading/download and dynamic address assignment are available on the specific server.

HTTP redirection

Whenever a user accesses the Internet through the Internet Explorer (IE) before passing 802.1x authentication, the device redirects the user to a predefined URL, such as the EAD client download interface.

With the above two functions of quick EAD deployment, the device redirects all users to a server to download and install the EAD client, resolving the EAD client deployment problem.



Note

The quick EAD deployment feature takes effect only when the authorization mode of an 802.1x-enabled port is set to **auto**.

Configuring Quick EAD Deployment

Configuration Prerequisites

- Enable 802.1x on the device.
- Set the port authorization mode to **auto** for 802.1x-enabled ports.

Configuration Procedure

Configuring a free IP range

A free IP range is an IP range that users can access before passing 802.1x authentication.

Follow these steps to configure a free IP range:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the URL for HTTP redirection	**dot1x url** *url-string*	Required
Configure a free IP range	**dot1x free-ip** *ip-address* { *mask-address* | *mask-length* }	Required By default, no free IP range is configured.

Caution

- You must configure the URL for HTTP redirection before configuring a free IP range. A URL must start with http:// and the segment where the URL resides must be in the free IP range. Otherwise, the redirection function cannot take effect.
- You must disable the DHCP-triggered authentication function of 802.1x before configuring a free IP range.
- With dot1x enabled but quick EAD deployment disabled, users cannot access the DHCP server if they fail 802.1x authentication. With quick EAD deployment enabled, users can obtain IP addresses dynamically before passing authentication if the IP address of the DHCP server is in the free IP range.
- The quick EAD deployment function applies to only ports with the authorization mode set to **auto** through the **dot1x port-control** command.
- Currently, the quick EAD deployment function is implemented based on only 802.1x authentication.
- Currently, the quick EAD deployment function does not support port security. The configured free IP range cannot take effect if you enable port security.

Setting the ACL timeout period

The quick EAD deployment function depends on ACLs in restricting access of users failing authentication. Each online user that has not passed authentication occupies a certain amount of ACL resources. After a user passes authentication, the occupied ACL resources will be released. When a large number of users log in but cannot pass authentication, the device may run out of ACL resources, preventing other users from logging in. A timer called ACL timer is designed to solve this problem.

You can control the usage of ACL resources by setting the ACL timer. The ACL timer starts once a user gets online. If the user has not passed authentication when the ACL timer expires, the occupied ACL resources are released for other users to use. If the device has a larger number of users, you can decrease the timeout period of the ACL timer appropriately for higher utilization of ACL resources.

Follow these steps to configure the ACL timer:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the ACL timer	**dot1x timer acl-timeout** *acl-timeout-value*	Required By default, the ACL timeout period is 30 minutes.

Displaying and Maintaining Quick EAD Deployment

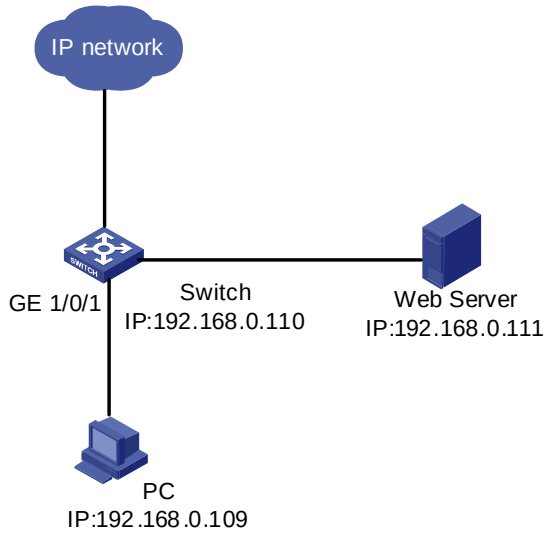
To do…	Use the command…	Remarks
Display configuration information about quick EAD deployment	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]	Available in any view.

Quick EAD Deployment Configuration Example

Network requirements

As shown in Figure 2-1, a user (PC) connects to the device (Switch) directly. The device connects to the Web server and the Internet. The user will be redirected to the Web server to download the authentication client and upgrade software when accessing the Internet through IE before passing authentication. After passing authentication, the user can access the Internet.

Figure 2-1 Network diagram for quick EAD deployment



Configuration procedure

Note

Before enabling quick EAD deployment, make sure that:

- The Web server is configured properly.
- The default gateway of the PC is configured as the IP address of the Layer-3 virtual interface of the VLAN to which the port that is directly connected with the PC belongs.

Configure the URL for HTTP redirection.

```
<device> system-view
[device] dot1x url http://192.168.0.111
```

Configure a free IP range.

```
[device] dot1x free-ip 192.168.0.111 24
```

Set the ACL timer to 10 minutes.

```
[device] dot1x timer acl-timeout 10
```

Enable dot1x globally.

```
[device] dot1x
```

Enable dot1x for GigabitEthernet 1/0/1.

```
[device] dot1x interface GigabitEthernet 1/0/1
```

Troubleshooting

Symptom: A user cannot be redirected to the specified URL server, no matter what URL the user enters in the IE address bar.

Solution:

- If a user enters an IP address in a format other than the dotted decimal notation, the user may not be redirected. This is related with the operating system used on the PC. In this case, the PC considers the IP address string a name and tries to resolve the name. If the resolution fails, the PC will access a specific website. Generally, this address is not in dotted decimal notation. As a result, the PC cannot receive any ARP response and therefore cannot be redirected. To solve this problem, the user needs to enter an IP address that is not in the free IP range in dotted decimal notation.
- If a user enters an address in the free IP range, the user cannot be redirected. This is because the device considers that the user wants to access a host in the free IP range. This is true even if no host with the IP address exists. To solve this problem, the user needs to enter an address not in the free IP range.
- Check that you have configured an IP address in the free IP range for the Web server and a correct URL for redirection, and that the server provides Web services properly.

3 System-Guard Configuration

System-Guard Overview

At first, you must determine whether the CPU is under attack to implement system guard for the CPU.

You should not determine whether the CPU is under attack just according to whether congestion occurs in a queue. Instead, you must do that in the following ways:

- According to the number of packets processed in the CPU in a time range.
- Or according to the time for one hundred packets to be processed.

If the CPU is under attack, the rate of packets to be processed in the CPU in a certain queue will exceed the threshold value. In this case, you can determine that the CPU is under attack. Through analyzing these packets, you get to know the characteristics of the attack source, and then you can adopt different filtering rules according the characteristics of the attack source. Thus, system guard is implemented.

Configuring the System-Guard Feature

Through the following configuration, you can enable the system-guard feature, set the threshold for the number of packets when an attack is detected and the length of the isolation after an attack is detected.

Configuring the System-Guard Feature

Follow these steps to configure the system-guard feature:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the system-guard feature	**system-guard enable**	Required By default, the system-guard feature is disabled.
Set the threshold for the number of packets when an attack is detected	**system-guard detect-threshold** *threshold-value*	Optional The default threshold value is 200 packets.
Set the length of the isolation after an attack is detected	**system-guard timer-interval** *isolate-timer*	Optional By default, the length of the isolation after an attack is detected is 10 minutes.

Displaying and Maintaining System-Guard

To do…	Use the command…	Remarks
Display the record of detected attacks	**display system-guard attack-record**	Available in any view
Display the state of the system-guard feature	**display system-guard state**	Available in any view

Table of Contents

1 AAA Overview 1-1
Introduction to AAA 1-1
Authentication 1-1
Authorization 1-1
Accounting 1-2
Introduction to ISP Domain 1-2
Introduction to AAA Services 1-2
Introduction to RADIUS 1-2
Introduction to HWTACACS 1-6

2 AAA Configuration 2-1
AAA Configuration Task List 2-1
Configuration Introduction 2-1
Creating an ISP Domain and Configuring Its Attributes 2-2
Configuring an AAA Scheme for an ISP Domain 2-3
Configuring Dynamic VLAN Assignment 2-5
Configuring the Attributes of a Local User 2-6
Cutting Down User Connections Forcibly 2-8
RADIUS Configuration Task List 2-8
Creating a RADIUS Scheme 2-10
Configuring RADIUS Authentication/Authorization Servers 2-10
Configuring RADIUS Accounting Servers 2-11
Configuring Shared Keys for RADIUS Messages 2-12
Configuring the Maximum Number of RADIUS Request Transmission Attempts 2-13
Configuring the Type of RADIUS Servers to be Supported 2-13
Configuring the Status of RADIUS Servers 2-14
Configuring the Attributes of Data to be Sent to RADIUS Servers 2-15
Configuring the Local RADIUS Authentication Server Function 2-16
Configuring Timers for RADIUS Servers 2-17
Enabling Sending Trap Message when a RADIUS Server Goes Down 2-18
Enabling the User Re-Authentication at Restart Function 2-18
HWTACACS Configuration Task List 2-19
Creating a HWTACACS Scheme 2-20
Configuring TACACS Authentication Servers 2-20
Configuring TACACS Authorization Servers 2-21
Configuring TACACS Accounting Servers 2-22
Configuring Shared Keys for HWTACACS Messages 2-22
Configuring the Attributes of Data to be Sent to TACACS Servers 2-23
Configuring the Timers Regarding TACACS Servers 2-24
Displaying and Maintaining AAA 2-25
AAA Configuration Examples 2-26
Remote RADIUS Authentication of Telnet/SSH Users 2-26
Local Authentication of FTP/Telnet Users 2-28
HWTACACS Authentication and Authorization of Telnet Users 2-29

Troubleshooting AAA ····· 2-30
Troubleshooting RADIUS Configuration ····· 2-30
Troubleshooting HWTACACS Configuration ····· 2-30
3 EAD Configuration ····· 3-1
Introduction to EAD ····· 3-1
Typical Network Application of EAD ····· 3-1
EAD Configuration ····· 3-2
EAD Configuration Example ····· 3-2

1 AAA Overview



Note

The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Introduction to AAA

AAA is the acronym for the three security functions: authentication, authorization and accounting. It provides a uniform framework for you to configure these three functions to implement network security management.

- Authentication: Defines what users can access the network,
- Authorization: Defines what services can be available to the users who can access the network, and
- Accounting: Defines how to charge the users who are using network resources.

Typically, AAA operates in the client/server model: the client runs on the managed resources side while the server stores the user information. Thus, AAA is well scalable and can easily implement centralized management of user information.

Authentication

AAA supports the following authentication methods:

- None authentication: Users are trusted and are not checked for their validity. Generally, this method is not recommended.
- Local authentication: User information (including user name, password, and some other attributes) is configured on this device, and users are authenticated on this device instead of on a remote device. Local authentication is fast and requires lower operational cost, but has the deficiency that information storage capacity is limited by device hardware.
- Remote authentication: Users are authenticated remotely through RADIUS or HWTACACS protocol. This device acts as the client to communicate with the RADIUS or TACACS server. You can use standard or extended RADIUS protocols in conjunction with such systems as iTELLIN/iMC for user authentication. Remote authentication allows convenient centralized management and is feature-rich. However, to implement remote authentication, a server is needed and must be configured properly.

Authorization

AAA supports the following authorization methods:

- Direct authorization: Users are trusted and directly authorized.

- Local authorization: Users are authorized according to the related attributes configured for their local accounts on this device.
- RADIUS authorization: Users are authorized after they pass RADIUS authentication. In RADIUS protocol, authentication and authorization are combined together, and authorization cannot be performed alone without authentication.
- HWTACACS authorization: Users are authorized by a TACACS server.

Accounting

AAA supports the following accounting methods:

- None accounting: No accounting is performed for users.
- Remote accounting: User accounting is performed on a remote RADIUS or TACACS server.

Introduction to ISP Domain

An Internet service provider (ISP) domain is a group of users who belong to the same ISP. For a user name in the format of userid@isp-name or userid.isp-name, the isp-name following the "@" or "." character is the ISP domain name. The access device uses userid as the user name for authentication, and isp-name as the domain name.

In a multi-ISP environment, the users connected to the same access device may belong to different domains. Since the users of different ISPs may have different attributes (such as different forms of user name and password, different service types/access rights), it is necessary to distinguish the users by setting ISP domains.

You can configure a set of ISP domain attributes (including AAA policy, RADIUS scheme, and so on) for each ISP domain independently in ISP domain view.

Introduction to AAA Services

Introduction to RADIUS

AAA is a management framework. It can be implemented by not only one protocol. But in practice, the most commonly used service for AAA is RADIUS.

What is RADIUS

RADIUS (remote authentication dial-in user service) is a distributed service based on client/server structure. It can prevent unauthorized access to your network and is commonly used in network environments where both high security and remote user access service are required.

The RADIUS service involves three components:

- Protocol: Based on the UDP/IP layer, RFC 2865 and 2866 define the message format and message transfer mechanism of RADIUS, and define 1812 as the authentication port and 1813 as the accounting port.
- Server: RADIUS Server runs on a computer or workstation at the center. It stores and maintains user authentication information and network service access information.
- Client: RADIUS Client runs on network access servers throughout the network.

RADIUS operates in the client/server model.

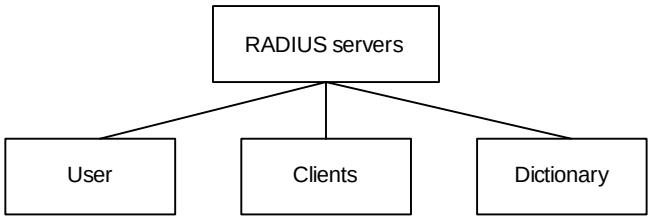
- A device acting as a RADIUS client passes user information to a specified RADIUS server, and takes appropriate action (such as establishing/terminating user connection) depending on the responses returned from the server.

- The RADIUS server receives user connection requests, authenticates users, and returns all required information to the device.

Generally, a RADIUS server maintains the following three databases (see Figure 1-1):

- Users: This database stores information about users (such as user name, password, protocol adopted and IP address).
- Clients: This database stores information about RADIUS clients (such as shared key).
- Dictionary: The information stored in this database is used to interpret the attributes and attribute values in the RADIUS protocol.

Figure 1-1 Databases in a RADIUS server

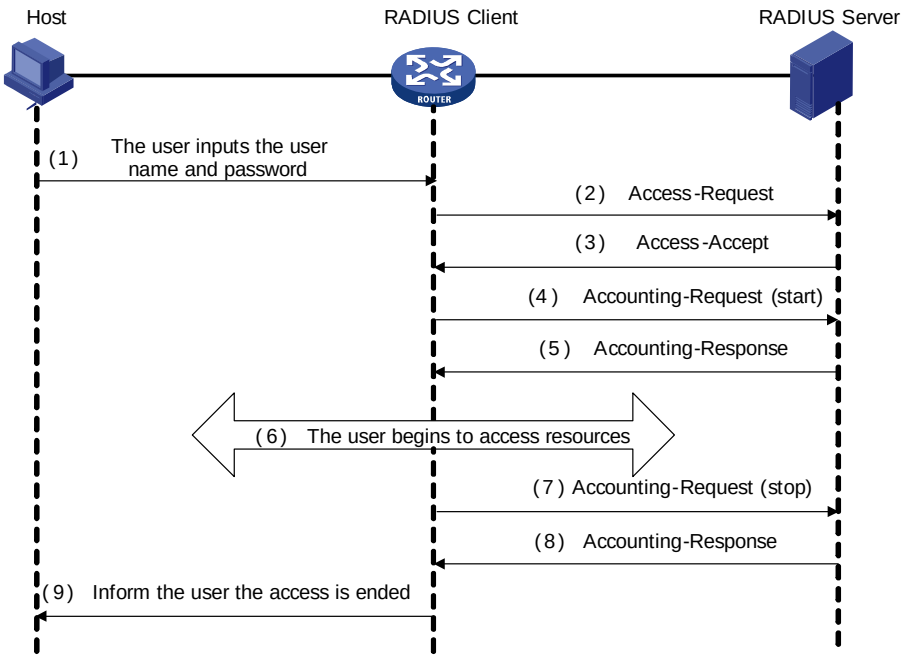


In addition, a RADIUS server can act as a client of some other AAA server to provide authentication or accounting proxy service.

Basic message exchange procedure in RADIUS

The messages exchanged between a RADIUS client and a RADIUS server are verified through a shared key. This enhances the security. The RADIUS protocol combines the authentication and authorization processes together by sending authorization information along with the authentication response message. Figure 1-2 depicts the message exchange procedure between the user, device and RADIUS server.

Figure 1-2 Basic message exchange procedure of RADIUS



The basic message exchange procedure of RADIUS is as follows:

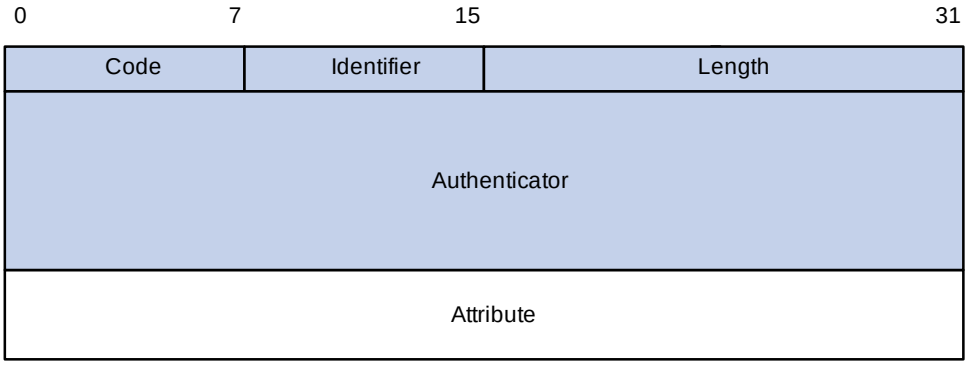
1) The user enters the user name and password.

2) The RADIUS client receives the user name and password, and then sends an authentication request (Access-Request) to the RADIUS server.
3) The RADIUS server compares the received user information with that in the Users database to authenticate the user. If the authentication succeeds, the RADIUS server sends back to the RADIUS client an authentication response (Access-Accept), which contains the user's authorization information. If the authentication fails, the server returns an Access-Reject response.
4) The RADIUS client accepts or denies the user depending on the received authentication result. If it accepts the user, the RADIUS client sends a start-accounting request (Accounting-Request, with the Status-Type attribute value = start) to the RADIUS server.
5) The RADIUS server returns a start-accounting response (Accounting-Response).
6) The user starts to access network resources.
7) The RADIUS client sends a stop-accounting request (Accounting-Request, with the Status-Type attribute value = stop) to the RADIUS server.
8) The RADIUS server returns a stop-accounting response (Accounting-Response).
9) The access to network resources is ended.

RADIUS message format

RADIUS messages are transported over UDP, which does not guarantee reliable delivery of messages between RADIUS server and client. As a remedy, RADIUS adopts the following mechanisms: timer management, retransmission, and backup server. Figure 1-3 depicts the format of RADIUS messages.

Figure 1-3 RADIUS message format



1) The Code field (one byte) decides the type of RADIUS message, as shown in Table 1-1.

Table 1-1 Description on the major values of the Code field

Code	Message type	Message description
1	Access-Request	Direction: client->server. The client transmits this message to the server to determine if the user can access the network. This message carries user information. It must contain the User-Name attribute and may contain the following attributes: NAS-IP-Address, User-Password and NAS-Port.
2	Access-Accept	Direction: server->client. The server transmits this message to the client if all the attribute values carried in the Access-Request message are acceptable (that is, the user passes the authentication).

Code	Message type	Message description
3	Access-Reject	Direction: server->client. The server transmits this message to the client if any attribute value carried in the Access-Request message is unacceptable (that is, the user fails the authentication).
4	Accounting-Request	Direction: client->server. The client transmits this message to the server to request the server to start or end the accounting (whether to start or to end the accounting is determined by the Acct-Status-Type attribute in the message). This message carries almost the same attributes as those carried in the Access-Request message.
5	Accounting-Response	Direction: server->client. The server transmits this message to the client to notify the client that it has received the Accounting-Request message and has correctly recorded the accounting information.

2) The Identifier field (one byte) is used to match requests and responses. It changes whenever the content of the Attributes field changes, and whenever a valid response has been received for a previous request, but remains unchanged for message retransmission.
3) The Length field (two bytes) specifies the total length of the message (including the Code, Identifier, Length, Authenticator and Attributes fields). The bytes beyond the length are regarded as padding and are ignored upon reception. If a received message is shorter than what the Length field indicates, it is discarded.
4) The Authenticator field (16 bytes) is used to authenticate the response from the RADIUS server; and is used in the password hiding algorithm. There are two kinds of authenticators: Request Authenticator and Response Authenticator.
5) The Attributes field contains specific authentication/authorization/accounting information to provide the configuration details of a request or response message. This field contains a list of field triplet (Type, Length and Value):

- The Type field (one byte) specifies the type of an attribute. Its value ranges from 1 to 255. Table 1-2 lists the attributes that are commonly used in RADIUS authentication/authorization.
- The Length field (one byte) specifies the total length of the attribute in bytes (including the Type, Length and Value fields).
- The Value field (up to 253 bytes) contains the information of the attribute. Its format is determined by the Type and Length fields.

Table 1-2 RADIUS attributes

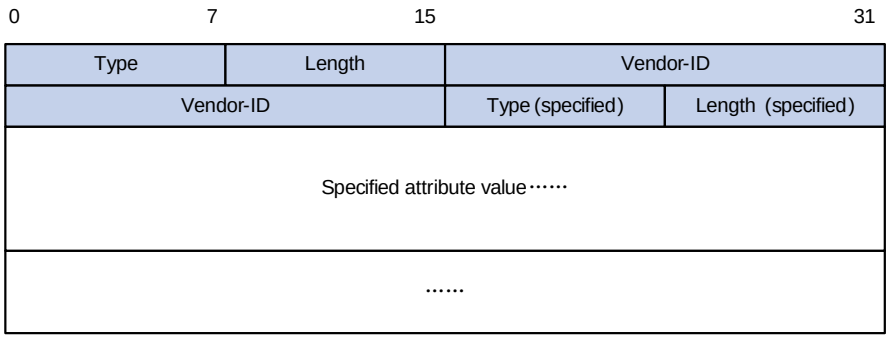
Type field value	Attribute type	Type field value	Attribute type
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action

Type field value	Attribute type	Type field value	Attribute type
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-ID	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-ID	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

The RADIUS protocol has good scalability. Attribute 26 (Vender-Specific) defined in this protocol allows a device vendor to extend RADIUS to implement functions that are not defined in standard RADIUS.

Figure 1-4 depicts the format of attribute 26. The Vendor-ID field used to identify a vendor occupies four bytes, where the first byte is 0, and the other three bytes are defined in RFC 1700. Here, the vendor can encapsulate multiple customized sub-attributes (containing vendor-specific Type, Length and Value) to implement a RADIUS extension.

Figure 1-4 Vendor-specific attribute format



Introduction to HWTACACS

What is HWTACACS

Huawei Terminal Access Controller Access Control System (HWTACACS) is an enhanced security protocol based on TACACS (RFC 1492). Similar to the RADIUS protocol, it implements AAA for different types of users (such as PPP, VPDN, and terminal users) through communicating with TACACS server in client-server mode.

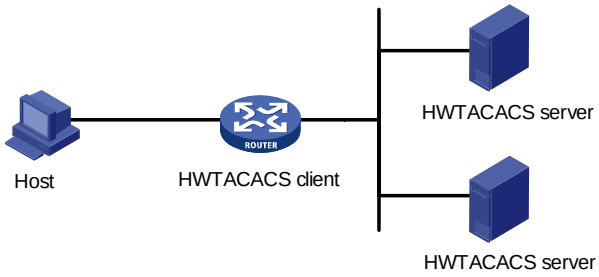
Compared with RADIUS, HWTACACS provides more reliable transmission and encryption, and therefore is more suitable for security control. Table 1-3 lists the primary differences between HWTACACS and RADIUS.

Table 1-3 Differences between HWTACACS and RADIUS

HWTACACS	RADIUS
Adopts TCP, providing more reliable network transmission.	Adopts UDP.
Encrypts the entire message except the HWTACACS header.	Encrypts only the password field in authentication message.
Separates authentication from authorization. For example, you can use one TACACS server for authentication and another TACACS server for authorization.	Combines authentication and authorization.
Is more suitable for security control.	Is more suitable for accounting.
Supports configuration command authorization.	Does not support.

In a typical HWTACACS application (as shown in Figure 1-5), a terminal user needs to log into the device to perform some operations. As a HWTACACS client, the device sends the username and password to the TACACS server for authentication. After passing authentication and being authorized, the user successfully logs into the switching engine to perform operations.

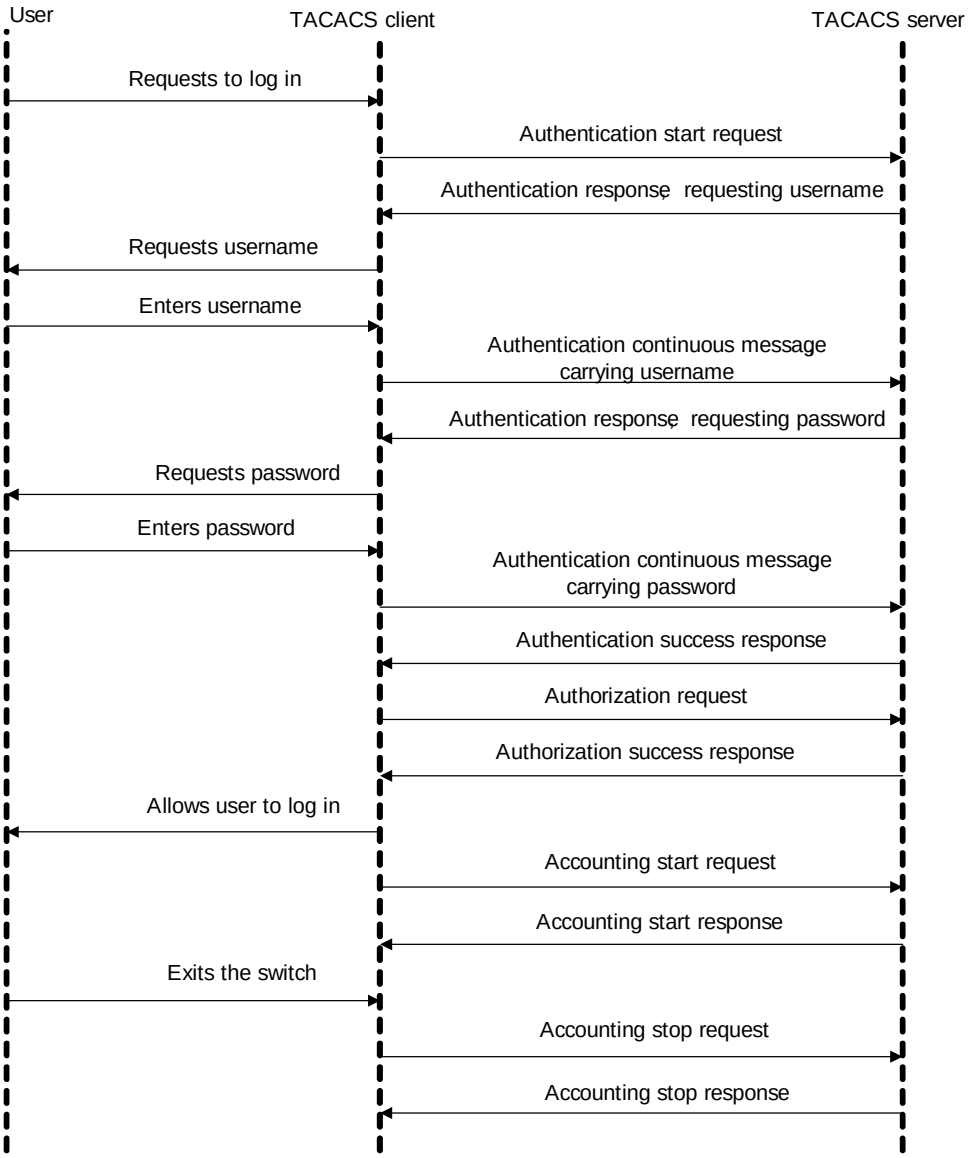
Figure 1-5 Network diagram for a typical HWTACACS application



Basic message exchange procedure in HWTACACS

The following text takes telnet user as an example to describe how HWTACACS implements authentication, authorization, and accounting for a user. Figure 1-6 illustrates the basic message exchange procedure:

Figure 1-6 AAA implementation procedure for a telnet user



The basic message exchange procedure is as follows:

1) A user sends a login request to the switching engine acting as a TACACS client, which then sends an authentication start request to the TACACS server.
2) The TACACS server returns an authentication response, asking for the username. Upon receiving the response, the TACACS client requests the user for the username.
3) After receiving the username from the user, the TACACS client sends an authentication continuance message carrying the username.
4) The TACACS server returns an authentication response, asking for the password. Upon receiving the response, the TACACS client requests the user for the login password.
5) After receiving the password, the TACACS client sends an authentication continuance message carrying the password to the TACACS server.
6) The TACACS server returns an authentication response, indicating that the user has passed the authentication.
7) The TACACS client sends a user authorization request to the TACACS server.
8) The TACACS server returns an authorization response, indicating that the user has passed the authorization.

9) After receiving the response indicating an authorization success, the TACACS client pushes the configuration interface of the device to the user.
10) The TACACS client sends an accounting start request to the TACACS server.
11) The TACACS server returns an accounting response, indicating that it has received the accounting start request.
12) The user logs out; the TACACS client sends an accounting stop request to the TACACS server.
13) The TACACS server returns an accounting response, indicating that it has received the accounting stop request.

2 AAA Configuration

AAA Configuration Task List

Configuration Introduction

You need to configure AAA to provide network access services for legal users while protecting network devices and preventing unauthorized access and repudiation behavior.

Complete the following tasks to configure a combined AAA scheme for an ISP domain:

Task			Remarks
AAA configuration	Creating an ISP Domain and Configuring Its Attributes		Required
	Configuring a combined AAA scheme		Required
	Configuring an AAA Scheme for an ISP Domain	None authentication	• Use one of the authentication methods • You need to configure RADIUS or HWATACACS before performing RADIUS or HWTACACS authentication
		Local authentication	
		RADIUS authentication	
		HWTACACS authentication	
	Configuring Dynamic VLAN Assignment		Optional
	Configuring the Attributes of a Local User		Optional
	Cutting Down User Connections Forcibly		Optional

Complete the following tasks to configure separate AAA schemes for an ISP domain:

Task		Remarks
AAA configuration	Creating an ISP Domain and Configuring Its Attributes	Required
	Configuring separate AAA schemes	Required
	Configuring an AAA Scheme for an ISP Domain	Required • With separate AAA schemes, you can specify authentication, authorization and accounting schemes respectively. • You need to configure RADIUS or HWATACACS before performing RADIUS or HWTACACS authentication.
	Configuring Dynamic VLAN Assignment	Optional
	Configuring the Attributes of a Local User	Optional
	Cutting Down User Connections Forcibly	Optional

Creating an ISP Domain and Configuring Its Attributes

Follow these steps to create an ISP domain and configure its attributes:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the form of the delimiter between the user name and the ISP domain name	**domain delimiter** { **at** | **dot** }	Optional By default, the delimiter between the user name and the ISP domain name is “@”.
Create an ISP domain or set an ISP domain as the default ISP domain	**domain** { *isp-name* | **default** { **disable** | **enable** *isp-name* } }	Required If no ISP domain is set as the default ISP domain, the ISP domain "system" is used as the default ISP domain.
Set the status of the ISP domain	**state** { **active** | **block** }	Optional By default, an ISP domain is in the **active** state, that is, all the users in the domain are allowed to request network service.
Set the maximum number of access users that the ISP domain can accommodate	**access-limit** { **disable** | **enable** *max-user-number* }	Optional By default, there is no limit on the number of access users that the ISP domain can accommodate.
Set the idle-cut function	**idle-cut** { **disable** | **enable** *minute flow* }	Optional By default, the idle-cut function is disabled.

To do…	Use the command…	Remarks
Set the accounting-optional switch	**accounting optional**	Optional By default, the accounting-optional switch is off.
Set the messenger function	**messenger time** { **enable** *limit interval* | **disable** }	Optional By default, the messenger function is disabled.
Set the self-service server location function	**self-service-url** { **disable** | **enable** *url-string* }	Optional By default, the self-service server location function is disabled.

Note that:

- On a unified device, each access user belongs to an ISP domain. You can configure up to 16 ISP domains on the device. When a user logs in, if no ISP domain name is carried in the user name, the device assumes that the user belongs to the default ISP domain.
- If you have configured to use "." as the delimiter, for a user name that contains multiple ".", the first "." will be used as the domain delimiter.
- If you have configured to use "@" as the delimiter, the "@" must not appear more than once in the user name.
- If the system does not find any available accounting server or fails to communicate with any accounting server when it performs accounting for a user, it does not disconnect the user as long as the accounting optional command has been executed, though it cannot perform accounting for the user in this case.
- The self-service server location function needs the cooperation of a RADIUS server that supports self-service, such as comprehensive access management server (iMC). Through self-service, users can manage and control their account or card numbers by themselves. A server installed with self-service software is called a self-service server.

Note

iMC Server is a service management system used to manage networks and ensure network and user information security. With the cooperation of other networking devices in a network, a iMC server can implement the AAA functions and right management.

Configuring an AAA Scheme for an ISP Domain

You can configure either of the following AAA schemes:

Configuring a combined AAA scheme

You can use the **scheme** command to specify an AAA scheme for an ISP domain. If you specify a RADIUS or HWTACACS scheme, the authentication, authorization and accounting will be uniformly implemented by the RADIUS or TACACS server(s) specified in the RADIUS or HWTACACS scheme. In

this way, you cannot specify different schemes for authentication, authorization and accounting respectively.

Follow these steps to configure a combined AAA scheme:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create an ISP domain and enter its view, or enter the view of an existing ISP domain	**domain** *isp-name*	Required
Configure an AAA scheme for the ISP domain	**scheme** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] }	Required By default, an ISP domain uses the **local** AAA scheme.

Caution

- You can execute the **scheme radius-scheme** *radius-scheme-name* command to adopt an already configured RADIUS scheme to implement all the three AAA functions. If you adopt the local scheme, only the authentication and authorization functions are implemented, the accounting function cannot be implemented.
- If you execute the **scheme radius-scheme** *radius-scheme-name* **local** command, the local scheme is used as the secondary scheme in case no RADIUS server is available. That is, if the communication between the device and a RADIUS server is normal, no local authentication is performed; otherwise, local authentication is performed.
- If you execute the **scheme hwtacacs-scheme** *hwtacacs-scheme-name* **local** command, the local scheme is used as the secondary scheme in case no TACACS server is available. That is, if the communication between the device and a TACACS server is normal, no local authentication is performed; otherwise, local authentication is performed.
- If you execute the **scheme local** or **scheme none** command to adopt **local** or **none** as the primary scheme, the local authentication is performed or no authentication is performed. In this case you cannot specify any RADIUS scheme or HWTACACS scheme at the same time.
- If you execute the scheme none command, the FTP users in the domain will not pass the authentication. So, to allow users to use the FTP service, you should not configure the none scheme.

Configuring separate AAA schemes

You can use the **authentication**, **authorization**, and **accounting** commands to specify a scheme for each of the three AAA functions (authentication, authorization and accounting) respectively. The following gives the implementations of this separate way for the services supported by AAA.

1) For terminal users

- Authentication: RADIUS, local, HWTACACS or none.
- Authorization: none or HWTACACS.
- Accounting: RADIUS, HWTACACS or none.

You can use an arbitrary combination of the above implementations for your AAA scheme configuration.

2) For FTP users

Only authentication is supported for FTP users.

Authentication: RADIUS, local, or HWTACACS.

Follow these steps to configure separate AAA schemes:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create an ISP domain and enter its view, or enter the view of an existing ISP domain	**domain** *isp-name*	Required
Configure an authentication scheme for the ISP domain	**authentication** { r**adius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** }	Optional By default, no separate authentication scheme is configured.
Configure an authorization scheme for the ISP domain	**authorization** { **none** | **hwtacacs-scheme** *hwtacacs-scheme-name* }	Optional By default, no separate authorization scheme is configured.
Configure an accounting scheme for the ISP domain	**accounting** { **none** | **radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* }	Optional By default, no separate accounting scheme is configured.

Note

- If a combined AAA scheme is configured as well as the separate authentication, authorization and accounting schemes, the separate ones will be adopted in precedence.
- RADIUS scheme and local scheme do not support the separation of authentication and authorization. Therefore, pay attention when you make authentication and authorization configuration for a domain: When the **scheme radius-scheme** or **scheme local** command is executed and the **authentication** command is not executed, the authorization information returned from the RADIUS or local scheme still takes effect even if the **authorization none** command is executed.

Configuring Dynamic VLAN Assignment

The dynamic VLAN assignment feature enables a device to dynamically add the ports of successfully authenticated users to different VLANs according to the attributes assigned by the RADIUS server, so as to control the network resources that different users can access.

Currently, the device supports the following two types of assigned VLAN IDs: integer and string.

- Integer: If the RADIUS authentication server assigns integer type of VLAN IDs, you can set the VLAN assignment mode to integer on the device (this is also the default mode on the device). Then,

upon receiving an integer ID assigned by the RADIUS authentication server, the device adds the port to the VLAN whose VLAN ID is equal to the assigned integer ID. If no such a VLAN exists, the device first creates a VLAN with the assigned ID, and then adds the port to the newly created VLAN.

- String: If the RADIUS authentication server assigns string type of VLAN IDs, you can set the VLAN assignment mode to string on the device. Then, upon receiving a string ID assigned by the RADIUS authentication server, the device compares the ID with existing VLAN names on the device. If it finds a match, it adds the port to the corresponding VLAN. Otherwise, the VLAN assignment fails and the user fails the authentication.

In actual applications, to use this feature together with Guest VLAN, you should better set port control to port-based mode. For more information, refer to the section discussing basic 802.1x configuration in *802.1x Operation.*

Follow these steps to configure dynamic VLAN assignment

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create an ISP domain and enter its view	**domain** i*sp-name*	—
Set the VLAN assignment mode	**vlan-assignment-mode** { **integer | string** }	Optional By default, the VLAN assignment mode is integer.
Create a VLAN and enter its view	**vlan** *vlan-id*	—
Set a VLAN name for VLAN assignment	**name** *string*	This operation is required if the VLAN assignment mode is set to string.

Caution

- In string mode, if the VLAN ID assigned by the RADIUS server is a character string containing only digits (for example, 1024), the device first regards it as an integer VLAN ID: the device transforms the string to an integer value and judges if the value is in the valid VLAN ID range; if it is, the device adds the authenticated port to the VLAN with the integer value as the VLAN ID (VLAN 1024, for example).
- To implement dynamic VLAN assignment on a port where both MSTP and 802.1x are enabled, you must set the MSTP port to an edge port.

Configuring the Attributes of a Local User

When **local** scheme is chosen as the AAA scheme, you should create local users on the device and configure the relevant attributes.

The local users are users set on the device, with each user uniquely identified by a user name. To make a user who is requesting network service pass local authentication, you should add an entry in the local user database on the device for the user.

Follow these steps to configure the attributes of a local user

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the password display mode of all local users	**local-user password-display-mode** { **cipher-force** | **auto** }	Optional By default, the password display mode of all access users is **auto**, indicating the passwords of access users are displayed in the modes set by the **password** command.
Add a local user and enter local user view	**local-user** *user-name*	Required By default, there is no local user in the system.
Set a password for the local user	**password** { **simple** | **cipher** } *password*	Required
Set the status of the local user	**state** { **active** | **block** }	Optional By default, the user is in **active** state, that is, the user is allowed to request network services.
Authorize the user to access specified type(s) of service	**service-type** { **ftp** | l**an-access** | { **telnet** | **ssh** | **terminal** }* [**level** *level*] }	Required By default, the system does not authorize the user to access any service.
Set the privilege level of the user	**level** *level*	Optional By default, the privilege level of the user is 0.
Configure the authorization VLAN for the local user	**authorization vlan** *string*	Required By default, no authorization VLAN is configured for the local user.
Set the attributes of the user whose service type is lan-access	**attribute** { **ip** *ip-address* | **mac** *mac-address* | **idle-cut** *second* | **access-limit** *max-user-number* | **vlan** *vlan-id* | **location** { **nas-ip** *ip-address* **port** *port-number* | **port** *port-number* } }*	Optional When binding the user to a remote port, you must use **nas-ip** *ip-address* to specify a remote access server IP address (here, *ip-address* is 127.0.0.1 by default, representing this device). When binding the user to a local port, you need not use **nas-ip** *ip-address*.

Caution

- The following characters are not allowed in the *user-name* string: /:*?<>. And you cannot input more than one "@" in the string.
- After the **local-user password-display-mode cipher-force** command is executed, any password will be displayed in cipher mode even though you specify to display a user password in plain text by using the **password** command.
- If a user name and password is required for user authentication (RADIUS authentication as well as local authentication), the command level that a user can access after login is determined by the privilege level of the user. For SSH users using RSA shared key for authentication, the commands they can access are determined by the levels set on their user interfaces.
- If the configured authentication method is none or password authentication, the command level that a user can access after login is determined by the level of the user interface.
- If the clients connected to a port have different authorization VLANs, only the first client passing the MAC address authentication can be assigned with an authorization VLAN. The device will not assign authorization VLANs for subsequent users passing MAC address authentication. In this case, you are recommended to connect only one MAC address authentication user or multiple users with the same authorization VLAN to a port.
- For local **RADIUS** authentication or **local** authentication to take effect, the VLAN assignment mode must be set to **string** after you specify authorization VLANs for local users.

Cutting Down User Connections Forcibly

Follow these steps to cut down user connections forcibly

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Cut down user connections forcibly	**cut connection** { **all** | **access-type** { **dot1x** | **mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name* }	Required

Note

You can use the **display connection** command to view the connections of Telnet users, but you cannot use the **cut connection** command to cut down their connections.

RADIUS Configuration Task List

The device can function not only as RADIUS clients but also as local RADIUS servers.

Complete the following tasks configure RADIUS for the device functioning as a RADIUS client:

Task		Remarks
Configuring the RADIUS client	Creating a RADIUS Scheme	Required
	Configuring RADIUS Authentication/Authorization Servers	Required
	Configuring RADIUS Accounting Servers	Required
	Configuring Shared Keys for RADIUS Messages	Optional
	Configuring the Maximum Number of RADIUS Request Transmission Attempts	Optional
	Configuring the Type of RADIUS Servers to be Supported	Optional
	Configuring the Status of RADIUS Servers	Optional
	Configuring the Attributes of Data to be Sent to RADIUS Servers	Optional
	Configuring Timers for RADIUS Servers	Optional
	Enabling Sending Trap Message when a RADIUS Server Goes Down	Optional
	Enabling the User Re-Authentication at Restart Function	Optional
Configuring the RADIUS server	Refer to the configuration of the RADIUS Server.	—

Complete the following tasks to configure RADIUS for the device functioning as a local RADIUS server:

Task		Remarks
Configuring the RADIUS server	Creating a RADIUS Scheme	Required
	Configuring RADIUS Authentication/Authorization Servers	Required
	Configuring RADIUS Accounting Servers	Required
	Configuring Shared Keys for RADIUS Messages	Optional
	Configuring the Maximum Number of RADIUS Request Transmission Attempts	Optional
	Configuring the Type of RADIUS Servers to be Supported	Optional
	Configuring the Status of RADIUS Servers	Optional
	Configuring the Attributes of Data to be Sent to RADIUS Servers	Optional
	Configuring the network access server and shared key enabled and allowed on the local RADIUS server	Required
	Configuring Timers for RADIUS Servers	Optional
	Enabling Sending Trap Message when a RADIUS Server Goes Down	Optional
Configuring the RADIUS client	Refer to the configuration of the RADIUS client	—

The RADIUS service configuration is performed on a RADIUS scheme basis. In an actual network environment, you can either use a single RADIUS server or two RADIUS servers (primary and

secondary servers with the same configuration but different IP addresses) in a RADIUS scheme. After creating a new RADIUS scheme, you should configure the IP address and UDP port number of each RADIUS server you want to use in this scheme. These RADIUS servers fall into two types: authentication/authorization, and accounting. And for each type of server, you can configure two servers in a RADIUS scheme: primary server and secondary server. A RADIUS scheme has some parameters such as IP addresses of the primary and secondary servers, shared keys, and types of the RADIUS servers.

In an actual network environment, you can configure the above parameters as required. But you should configure at least one authentication/authorization server and one accounting server, and you should keep the RADIUS server port settings on the device consistent with those on the RADIUS servers.

 **Note**

Actually, the RADIUS service configuration only defines the parameters for information exchange between device and RADIUS server. To make these parameters take effect, you must reference the RADIUS scheme configured with these parameters in an ISP domain view (refer to AAA Configuration).

Creating a RADIUS Scheme

The RADIUS protocol configuration is performed on a RADIUS scheme basis. You should first create a RADIUS scheme and enter its view before performing other RADIUS protocol configurations.

Follow these steps to create a RADIUS scheme:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable RADIUS authentication port	**radius client enable**	Optional By default, RADIUS authentication port is enabled.
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.

 **Note**

A RADIUS scheme can be referenced by multiple ISP domains simultaneously.

Configuring RADIUS Authentication/Authorization Servers

Follow these steps to configure RADIUS authentication/authorization servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the IP address and port number of the primary RADIUS authentication/authorization server	**primary authentication** *ip-address* [*port-number*]	Required By default, the IP address and UDP port number of the primary server are 0.0.0.0 and 1812 respectively for a newly created RADIUS scheme.
Set the IP address and port number of the secondary RADIUS authentication/authorization server	**secondary authentication** *ip-address* [*port-number*]	Optional By default, the IP address and UDP port number of the secondary server are 0.0.0.0 and 1812 respectively for a newly created RADIUS scheme.

Note

- The authentication response sent from the RADIUS server to the RADIUS client carries authorization information. Therefore, you need not (and cannot) specify a separate RADIUS authorization server.
- In an actual network environment, you can specify one server as both the primary and secondary authentication/authorization servers, as well as specifying two RADIUS servers as the primary and secondary authentication/authorization servers respectively.
- The IP address and port number of the primary authentication server used by the default RADIUS scheme "system" are 127.0.0.1 and 1645.

Configuring RADIUS Accounting Servers

Follow these steps to configure RADIUS accounting servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the IP address and port number of the primary RADIUS accounting server	**primary accounting** *ip-address* [*port-number*]	Required By default, the IP address and UDP port number of the primary accounting server are 0.0.0.0 and 1813 for a newly created RADIUS scheme.

To do…	Use the command…	Remarks
Set the IP address and port number of the secondary RADIUS accounting server	**secondary accounting** *ip-address* [*port-number*]	Optional By default, the IP address and UDP port number of the secondary accounting server are 0.0.0.0 and 1813 for a newly created RADIUS scheme.
Enable stop-accounting request buffering	**stop-accounting-buffer enable**	Optional By default, stop-accounting request buffering is enabled.
Set the maximum number of transmission attempts of a buffered stop-accounting request.	**retry stop-accounting** *retry-times*	Optional By default, the system tries at most 500 times to transmit a buffered stop-accounting request.
Set the maximum allowed number of continuous real-time accounting failures	**retry realtime-accounting** *retry-times*	Optional By default, the maximum allowed number of continuous real-time accounting failures is five. If five continuous failures occur, the device cuts down the user connection.

Note

- In an actual network environment, you can specify one server as both the primary and secondary accounting servers, as well as specifying two RADIUS servers as the primary and secondary accounting servers respectively. In addition, because RADIUS adopts different UDP ports to exchange authentication/authorization messages and accounting messages, you must set a port number for accounting different from that set for authentication/authorization.
- With stop-accounting request buffering enabled, the device first buffers the stop-accounting request that gets no response from the RADIUS accounting server, and then retransmits the request to the RADIUS accounting server until it gets a response, or the maximum number of transmission attempts is reached (in this case, it discards the request).
- You can set the maximum allowed number of continuous real-time accounting failures. If the number of continuously failed real-time accounting requests to the RADIUS server reaches the set maximum number, the device cuts down the user connection.
- The IP address and port number of the primary accounting server of the default RADIUS scheme "system" are 127.0.0.1 and 1646 respectively.
- Currently, RADIUS does not support the accounting of FTP users.

Configuring Shared Keys for RADIUS Messages

Both RADIUS client and server adopt MD5 algorithm to encrypt RADIUS messages before they are exchanged between the two parties. The two parties verify the validity of the RADIUS messages

received from each other by using the shared keys that have been set on them, and can accept and respond to the messages only when both parties have the same shared key.

Follow these steps to configure shared keys for RADIUS messages:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set a shared key for RADIUS authentication/authorization messages	**key authentication** *string*	Required By default, no shared key is created.
Set a shared key for RADIUS accounting messages	**key accounting** *string*	Required By default, no shared key is created.

Caution

The authentication/authorization shared key and the accounting shared key you set on the device must be respectively consistent with the shared key on the authentication/authorization server and the shared key on the accounting server.

Configuring the Maximum Number of RADIUS Request Transmission Attempts

The communication in RADIUS is unreliable because this protocol uses UDP packets to carry its data. Therefore, it is necessary for the device to retransmit a RADIUS request if it gets no response from the RADIUS server after the response timeout timer expires. If the device gets no answer after it has tried the maximum number of times to transmit the request, the device considers that the request fails.

Follow these steps to configure the maximum transmission attempts of a RADIUS request:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the maximum number of RADIUS request transmission attempts	**retry** *retry-times*	Optional By default, the system can try three times to transmit a RADIUS request.

Configuring the Type of RADIUS Servers to be Supported

Follow these steps to configure the type of RADIUS servers to be supported:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Configure the type of RADIUS servers to be supported	**server-type** { **extended** | **standard** }	Optional

Note

When the third party RADIUS server is used, you can select **standard** or **extended** as the server-type in a RADIUS scheme; when the iMC server is used, you can select **extended** as the server-type in a RADIUS scheme.

Configuring the Status of RADIUS Servers

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme:

When the device fails to communicate with the primary server due to some server trouble, the device will turn to the secondary server and exchange messages with the secondary server.

After the primary server remains in the **block** state for a set time (set by the **timer quiet** command), the device will try to communicate with the primary server again when it receives a RADIUS request. If it finds that the primary server has recovered, the device immediately restores the communication with the primary server instead of communicating with the secondary server, and at the same time restores the status of the primary server to **active** while keeping the status of the secondary server unchanged.

When both the primary and secondary servers are in **active** or **block** state, the device sends messages only to the primary server.

Follow these steps to set the status of RADIUS servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.

To do…	Use the command…	Remarks
Set the status of the primary RADIUS authentication/authorization server	**state primary authentication** { **block** | **active** }	Optional By default, the primary RADIUS servers in the default RADIUS scheme "system" are in the **active** state, the secondary servers in the scheme are in the **block** state, and all RADIUS servers in all other RADIUS schemes are in the **block** state.
Set the status of the primary RADIUS accounting server	**state primary accounting** { **block** | **active** }	
Set the status of the secondary RADIUS authentication/authorization server	**state secondary authentication** { **block** | **active** }	
Set the status of the secondary RADIUS accounting server	**state secondary accounting** { **block** | **active** }	

Configuring the Attributes of Data to be Sent to RADIUS Servers

Follow these steps to configure the attributes of data to be sent to RADIUS servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the format of the user names to be sent to RADIUS server	**user-name-format** { **with-domain** | **without-domain** }	Optional By default, the user names sent from the device to RADIUS server carry ISP domain names.
Set the units of data flows to RADIUS servers	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-packet** | **kilo-packet** | **mega- packet** | **one-packet** }	Optional By default, in a RADIUS scheme, the data unit and packet unit for outgoing RADIUS flows are byte and one-packet respectively.
Set the MAC address format of the Calling-Station-Id (Type 31) field in RADIUS packets	**calling-station-id mode** { **mode1** | **mode2** } { **lowercase** | **uppercase** }	Optional By default, the MAC address format is XXXX-XXXX-XXXX, in lowercase.
Set the source IP address of outgoing RADIUS messages	RADIUS scheme view **nas-ip** *ip-address*	Optional By default, no source IP address is set; and the IP address of the corresponding outbound interface is used as the source IP address.
	System view **radius nas-ip** *ip-address*	

Note

- Generally, the access users are named in the *userid@isp-name* or *userid.isp-name* format. Here, *isp-name* after the "@" or "." character represents the ISP domain name, by which the device determines which ISP domain a user belongs to. However, some old RADIUS servers cannot accept the user names that carry ISP domain names. In this case, it is necessary to remove domain names from user names before sending the user names to RADIUS server. For this reason, the **user-name-format** command is designed for you to specify whether or not ISP domain names are carried in the user names to be sent to RADIUS server.
- For a RADIUS scheme, if you have specified to remove ISP domain names from user names, you should not use this RADIUS scheme in more than one ISP domain. Otherwise, such errors may occur: the RADIUS server regards two different users having the same name but belonging to different ISP domains as the same user (because the usernames sent to it are the same).
- In the default RADIUS scheme "system", ISP domain names are removed from user names by default.
- The purpose of setting the MAC address format of the Calling-Station-Id (Type 31) field in RADIUS packets is to improve the device's compatibility with different RADIUS servers. This setting is necessary when the format of Calling-Station-Id field recognizable to RADIUS servers is different from the default MAC address format on the device. For details about field formats recognizable to RADIUS servers, refer to the corresponding RADIUS server manual.

Configuring the Local RADIUS Authentication Server Function

The device provides the local RADIUS server function (including authentication and authorization), also known as the local RADIUS authentication server function, in addition to RADIUS client service, where separate authentication/authorization server and the accounting server are used for user authentication.

Follow these steps to configure the local RADIUS authentication server function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable UDP port for local RADIUS authentication server	**local-server enable**	Optional By default, the UDP port for local RADIUS authentication server is enabled.
Configure the parameters of the local RADIUS server	**local-server nas-ip** *ip-address* **key** *password*	Required By default, a local RADIUS authentication server is configured with an NAS IP address of 127.0.0.1.

Caution

- If you adopt the local RADIUS authentication server function, the UDP port number of the authentication/authorization server must be 1645, the UDP port number of the accounting server must be 1646, and the IP addresses of the servers must be set to the addresses of this device.
- The message encryption key set by the **local-server nas-ip** *ip-address* **key** *password* command must be identical with the authentication/authorization message encryption key set by the **key authentication** command in the RADIUS scheme view of the RADIUS scheme on the specified NAS that uses this device as its authentication server.
- The device supports IP addresses and shared keys for up to 16 network access servers (NAS). That is, when acting as the local RADIUS authentication server, the device can provide authentication service to up to 16 network access servers (including the device itself) at the same time.
- When acting as the local RADIUS authentication server, the device does not support EAP authentication.

Configuring Timers for RADIUS Servers

After sending out a RADIUS request (authentication/authorization request or accounting request) to a RADIUS server, the device waits for a response from the server. The maximum time that the device can wait for the response is called the response timeout time of RADIUS servers, and the corresponding timer in the device system is called the response timeout timer of RADIUS servers. If the device gets no answer within the response timeout time, it needs to retransmit the request to ensure that the user can obtain RADIUS service.

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme:

When the device fails to communicate with the primary server due to some server trouble, the device will turn to the secondary server and exchange messages with the secondary server.

After the primary server remains in the **block** state for a specific time (set by the **timer quiet** command), the device will try to communicate with the primary server again when it has a RADIUS request. If it finds that the primary server has recovered, the device immediately restores the communication with the primary server instead of communicating with the secondary server, and at the same time restores the status of the primary server to **active** while keeping the status of the secondary server unchanged.

To control the interval at which users are charged in real time, you can set the real-time accounting interval. After the setting, the device periodically sends online users' accounting information to RADIUS server at the set interval.

Follow these steps to set timers for RADIUS servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.

To do…	Use the command…	Remarks
Set the response timeout time of RADIUS servers	**timer response-timeout** *seconds*	Optional By default, the response timeout time of RADIUS servers is three seconds.
Set the time that the device waits before it try to re-communicate with primary server and restore the status of the primary server to active	**timer quiet** *minutes*	Optional By default, the device waits five minutes before it restores the status of the primary server to active.
Set the real-time accounting interval	**timer realtime-accounting** *minutes*	Optional By default, the real-time accounting interval is 12 minutes.

Enabling Sending Trap Message when a RADIUS Server Goes Down

Follow these steps to specify to send trap message when a RADIUS server goes down:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the sending of trap message when a RADIUS server is down	**radius trap** { **authentication-server-down** **| accounting-server-down** }	Optional By default, the device does not send trap message when a RADIUS server is down.

Note

- This configuration takes effect on all RADIUS schemes.
- The device considers a RADIUS server as being down if it has tried the configured maximum times to send a message to the RADIUS server but does not receive any response.

Enabling the User Re-Authentication at Restart Function

Note

The user re-authentication at restart function applies only to the environment where the RADIUS authentication/authorization and accounting server is iMC.

In an environment that a iMC server is used to implement AAA functions, if the device reboots after an exclusive user (a user whose concurrent online number is set to 1 on the iMC) gets authenticated and authorized and begins being charged, the device will give a prompt that the user has already been

online when the user re-logs into the switching engine before the iMC performs online user detection, and the user cannot get authenticated. In this case, the user can access the network again only when the iMC administrator manually removes the user's online information.

The user re-authentication at restart function is designed to resolve this problem. After this function is enabled, every time the device restarts:

1) The device generates an Accounting-On message, which mainly contains the following information: NAS-ID, NAS-IP-address (source IP address), and session ID.
2) The device sends the Accounting-On message to the IMC at regular intervals.
3) Once the IMC receives the Accounting-On message, it sends a response to the device. At the same time it finds and deletes the original online information of the users who were accessing the network through the device before the restart according to the information (NAS-ID, NAS-IP-address and session ID) contained in the message, and ends the accounting for the users depending on the last accounting update message.
4) Once the device receives the response from the IMC, it stops sending Accounting-On messages.
5) If the device does not receive any response from the IMC after it has tried the configured maximum number of times to send the Accounting-On message, it will not send the Accounting-On message any more.

 **Note**

The device can automatically generate the main attributes (NAS-ID, NAS-IP-address and session ID) contained in Accounting-On messages. However, you can also manually configure the NAS-IP-address with the **nas-ip** command. If you choose to manually configure the attribute, be sure to configure an appropriate valid IP address. If this attribute is not configured, the device will automatically choose the IP address of a VLAN interface as the NAS-IP-address.

Follow these steps to enable the user re-authentication at restart function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter RADIUS scheme view	**radius scheme** *radius-scheme-name*	—
Enable the user re-authentication at restart function	**accounting-on enable** [**send** *times* | **interval** *interval*]	By default, this function is disabled. If you use this command without any parameter, the system will try at most 15 times to send an Accounting-On message at the interval of three seconds.

HWTACACS Configuration Task List

Complete the following tasks to configure HWTACACS:

Task		Remarks
Configuring the TACACS client	Creating a HWTACACS Scheme	Required
	Configuring TACACS Authentication Servers	Required
	Configuring TACACS Authorization Servers	Required
	Configuring TACACS Accounting Servers	Optional
	Configuring Shared Keys for RADIUS Messages	Optional
	Configuring the Attributes of Data to be Sent to TACACS Servers	Optional
	Configuring the Timers Regarding TACACS Servers	Optional
Configuring the TACACS server	Refer to the configuration of TACACS servers.	—

Creating a HWTACACS Scheme

The HWTACACS protocol configuration is performed on a scheme basis. Therefore, you must create a HWTACACS scheme and enter HWTACACS view before performing other configuration tasks.

Follow these steps to create a HWTACACS scheme:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.

Caution

The system supports up to 16 HWTACACS schemes. You can delete a HWTACACS scheme only when it is not referenced.

Configuring TACACS Authentication Servers

Follow these steps to configure TACACS authentication servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.

To do…	Use the command…	Remarks
Set the IP address and port number of the primary TACACS authentication server	**primary authentication** *ip-address* [*port*]	Required By default, the IP address of the primary authentication server is 0.0.0.0, and the port number is 0.
Set the IP address and port number of the secondary TACACS authentication server	**secondary authentication** *ip-address* [*port*]	Optional By default, the IP address of the secondary authentication server is 0.0.0.0, and the port number is 0.

Caution

- You are not allowed to configure the same IP address for both primary and secondary authentication servers. If you do this, the system will prompt that the configuration fails.
- You can remove an authentication server setting only when there is no active TCP connection that is sending authentication messages to the server.

Configuring TACACS Authorization Servers

Follow these steps to configure TACACS authorization servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the IP address and port number of the primary TACACS authorization server	**primary authorization** *ip-address* [*port*]	Required By default, the IP address of the primary authorization server is 0.0.0.0, and the port number is 0.
Set the IP address and port number of the secondary TACACS authorization server	**secondary authorization** *ip-address* [*port*]	Optional By default, the IP address of the secondary authorization server is 0.0.0.0, and the port number is 0.

Caution

- You are not allowed to configure the same IP address for both primary and secondary authorization servers. If you do this, the system will prompt that the configuration fails.
- You can remove a server only when it is not used by any active TCP connection for sending authorization messages.

Configuring TACACS Accounting Servers

Follow these steps to configure TACACS accounting servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the IP address and port number of the primary TACACS accounting server	**primary accounting** *ip-address* [*port*]	Required By default, the IP address of the primary accounting server is 0.0.0.0, and the port number is 0.
Set the IP address and port number of the secondary TACACS accounting server	**secondary accounting** *ip-address* [*port*]	Required By default, the IP address of the secondary accounting server is 0.0.0.0, and the port number is 0.
Enable the stop-accounting message retransmission function and set the maximum number of transmission attempts of a buffered stop-accounting message	**retry stop-accounting** *retry-times*	Optional By default, the stop-accounting messages retransmission function is enabled and the system can transmit a buffered stop-accounting request for 100 times.

Caution

- You are not allowed to configure the same IP address for both primary and secondary accounting servers. If you do this, the system will prompt that the configuration fails.
- You can remove a server only when it is not used by any active TCP connection for sending accounting messages.

Configuring Shared Keys for HWTACACS Messages

When using a TACACS server as an AAA server, you can set a key to improve the communication security between the device and the TACACS server.

The TACACS client and server adopt MD5 algorithm to encrypt HWTACACS messages before they are exchanged between the two parties. The two parties verify the validity of the HWTACACS messages received from each other by using the shared keys that have been set on them, and can accept and respond to the messages only when both parties have the same shared key.

Follow these steps to configure shared keys for HWTACACS messages:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set a shared key for HWTACACS authentication, authorization or accounting messages	**key** { **accounting** | **authorization** | **authentication** } *string*	Required By default, no such key is set.

Configuring the Attributes of Data to be Sent to TACACS Servers

Follow these steps to configure the attributes for data to be sent to TACACS servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the format of the user names to be sent to TACACS server	**user-name-format** { **with-domain** | **without-domain** }	Optional By default, the user names sent from the device to TACACS server carry ISP domain names.
Set the units of data flows to TACACS servers	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }	Optional By default, in a TACACS scheme, the data unit and packet unit for outgoing HWTACACS flows are byte and one-packet respectively.
	data-flow-format packet { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }	
Set the source IP address of outgoing HWTACACS messages	HWTACACS scheme view **nas-ip** *ip-address*	Optional By default, no source IP address is set; the IP address of the corresponding outbound interface is used as the source IP address.
	System view **hwtacacs nas-ip** *ip-address*	

Caution

Generally, the access users are named in the *userid@isp-name* or *userid.isp-name* format. Where, *isp-name* after the "@" or "." character represents the ISP domain name. If the TACACS server does not accept the user names that carry ISP domain names, it is necessary to remove domain names from user names before they are sent to TACACS server.

Configuring the Timers Regarding TACACS Servers

Follow these steps to configure the timers regarding TACACS servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the response timeout time of TACACS servers	**timer response-timeout** *seconds*	Optional By default, the response timeout time is five seconds.
Set the time that the device must wait before it can restore the status of the primary server to active	**timer quiet** *minutes*	Optional By default, the device must wait five minutes before it can restore the status of the primary server to active.
Set the real-time accounting interval	**timer realtime-accounting** *minutes*	Optional By default, the real-time accounting interval is 12 minutes.

Caution

- To control the interval at which users are charge in real time, you can set the real-time accounting interval. After the setting, the device periodically sends online users' accounting information to the TACACS server at the set interval.
- The real-time accounting interval must be a multiple of 3.
- The setting of real-time accounting interval somewhat depends on the performance of the TACACS client and server devices: A shorter interval requires higher device performance.

Displaying and Maintaining AAA

Displaying and maintaining AAA information

To do…	Use the command…	Remarks
Display configuration information about one specific or all ISP domains	**display domain** [*isp-name*]	Available in any view.
Display information about user connections	**display connection** [**access-type** { **dot1x** **|** **mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name*]	
Display information about local users	**display local-user** [**domain** *isp-name* | **idle-cut** { **disable** | **enable** } | **vlan** *vlan-id* | **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name*]	

Displaying and maintaining RADIUS protocol information

To do…	Use the command…	Remarks
Display RADIUS message statistics about local RADIUS authentication server	**display local-server statistics**	Available in any view.
Display configuration information about one specific or all RADIUS schemes	**display radius scheme** [*radius-scheme-name*]	
Display RADIUS message statistics	**display radius statistics**	
Display buffered non-response stop-accounting requests	**display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	
Delete buffered non-response stop-accounting requests	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	Available in user view.
Clear RADIUS message statistics	**reset radius statistics**	

Displaying and maintaining HWTACACS protocol information

To do…	Use the command…	Remarks
Display the configuration or statistic information about one specific or all HWTACACS schemes	**display hwtacacs** [*hwtacacs-scheme-name* [**statistics**]]	Available in any view.
Display buffered non-response stop-accounting requests	**display stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name*	
Clear HWTACACS message statistics	**reset hwtacacs statistics** { **accounting** | **authentication** | **authorization** | **all** }	Available in user view.
Delete buffered non-response stop-accounting requests	**reset stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name*	

AAA Configuration Examples

Remote RADIUS Authentication of Telnet/SSH Users

Note

The configuration procedure for remote authentication of SSH users by RADIUS server is similar to that for Telnet users. The following text only takes Telnet users as example to describe the configuration procedure for remote authentication.

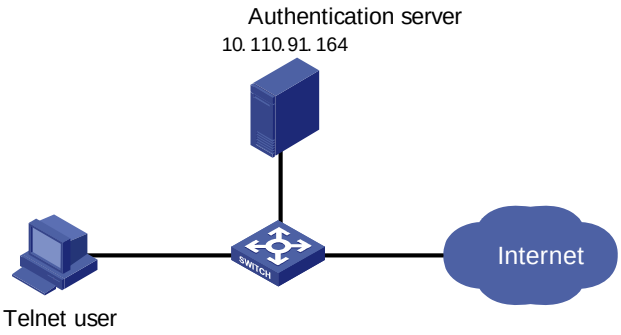
Network requirements

In the network environment shown in Figure 2-1, you are required to configure the device so that the Telnet users logging into the switching engine are authenticated by the RADIUS server.

- A RADIUS authentication server with IP address 10.110.91.164 is connected to the device.
- On the device, set the shared key it uses to exchange messages with the authentication RADIUS server to "aabbcc".
- A IMC server is used as the RADIUS server. You can select **extended** as the server-type in a RADIUS scheme.
- On the RADIUS server, set the shared key it uses to exchange messages with the device to "aabbcc," set the authentication port number, and add Telnet user names and login passwords.

The Telnet user names added to the RADIUS server must be in the format of *userid@isp-name* if you have configured the device to include domain names in the user names to be sent to the RADIUS server in the RADIUS scheme.

Figure 2-1 Remote RADIUS authentication of Telnet users



Configuration procedure

Enter system view.

```
<device> system-view
```

Adopt AAA authentication for Telnet users.

```
[device] user-interface vty 0 4
[device-ui-vty0-4] authentication-mode scheme
[device-ui-vty0-4] quit
```

Configure an ISP domain.

```
[device] domain imc
[device-isp-imc] access-limit enable 10
[device-isp-imc] quit
```

Configure a RADIUS scheme.

```
[device] radius scheme imc
[device-radius-imc] accounting optional
[device-radius-imc] primary authentication 10.110.91.164 1812
[device-radius-imc] key authentication aabbcc
[device-radius-imc] server-type Extended
[device-radius-imc] user-name-format with-domain
[device-radius-imc] quit
```

Associate the ISP domain with the RADIUS scheme.

```
[device] domain imc
[device-isp-imc] scheme radius-scheme imc
```

A Telnet user logging into the device by a name in the format of *userid* @imc belongs to the imc domain and will be authenticated according to the configuration of the imc domain.

Local Authentication of FTP/Telnet Users

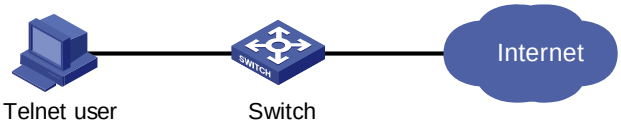
Note

The configuration procedure for local authentication of FTP users is similar to that for Telnet users. The following text only takes Telnet users as example to describe the configuration procedure for local authentication.

Network requirements

In the network environment shown in Figure 2-2, you are required to configure the device so that the Telnet users logging into the switching engine are authenticated locally.

Figure 2-2 Local authentication of Telnet users



Configuration procedure

Method 1: Using local authentication scheme.

Enter system view.

```
<device> system-view
```

Adopt AAA authentication for Telnet users.

```
[device] user-interface vty 0 4
[device-ui-vty0-4] authentication-mode scheme
[device-ui-vty0-4] quit
```

Create and configure a local user named "telnet".

```
[device] local-user telnet
[device-luser-telnet] service-type telnet
[device-luser-telnet] password simple aabbcc
[device-luser-telnet] quit
```

Configure an authentication scheme for the default “system” domain.

```
[device] domain system
[device-isp-system] scheme local
```

A Telnet user logging into the device with the name telnet@system belongs to the "system" domain and will be authenticated according to the configuration of the "system" domain.

Method 2: using local RADIUS server

This method is similar to the remote authentication method described in Remote RADIUS Authentication of Telnet/SSH Users. However, you need to

- Change the server IP address, and the UDP port number of the authentication server to 127.0.0.1, and 1645 respectively in the configuration step "Configure a RADIUS scheme" in Remote RADIUS Authentication of Telnet/SSH Users
- Enable the local RADIUS server function, set the IP address and shared key for the network access server to 127.0.0.1 and aabbcc, respectively.
- Configure local users.

HWTACACS Authentication and Authorization of Telnet Users

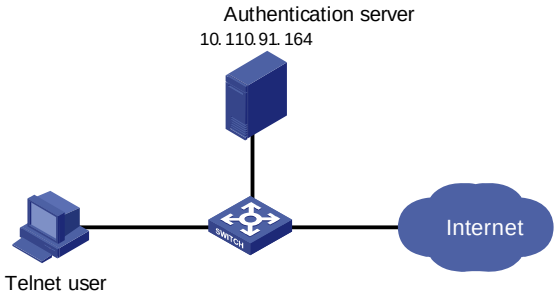
Network requirements

You are required to configure the device so that the Telnet users logging into the switching engine are authenticated and authorized by the TACACS server.

A TACACS server with IP address 10.110.91.164 is connected to the device. This server will be used as the authentication and authorization server. On the device, set both authentication and authorization shared keys that are used to exchange messages with the TACACS server to "expert." Configure the device to strip domain names off user names before sending user names to the TACACS server.

Configure the shared key to “expert” on the TACACS server for exchanging messages with the device.

Figure 2-3 Remote HWTACACS authentication and authorization of Telnet users



Configuration procedure

Add a Telnet user.

(Omitted here)

Configure a HWTACACS scheme.

```
<device> system-view
[device] hwtacacs scheme hwtac
[device-hwtacacs-hwtac] primary authentication 10.110.91.164 49
[device-hwtacacs-hwtac] primary authorization 10.110.91.164 49
[device-hwtacacs-hwtac] key authentication expert
[device-hwtacacs-hwtac] key authorization expert
[device-hwtacacs-hwtac] user-name-format without-domain
[device-hwtacacs-hwtac] quit
```

Configure the domain name of the HWTACACS scheme to hwtac.

```
[device] domain hwtacacs
[device-isp-hwtacacs] scheme hwtacacs-scheme hwtac
```

Troubleshooting AAA

Troubleshooting RADIUS Configuration

The RADIUS protocol operates at the application layer in the TCP/IP protocol suite. This protocol prescribes how the device and the RADIUS server of the ISP exchange user information with each other.

Symptom 1: User authentication/authorization always fails.

Possible reasons and solutions:

- The user name is not in the userid@isp-name or *userid.isp-name* format, or the default ISP domain is not correctly specified on the device — Use the correct user name format, or set a default ISP domain on the device.
- The user is not configured in the database of the RADIUS server — Check the database of the RADIUS server, make sure that the configuration information about the user exists.
- The user input an incorrect password — Be sure to input the correct password.
- The device and the RADIUS server have different shared keys — Compare the shared keys at the two ends, make sure they are identical.
- The device cannot communicate with the RADIUS server (you can determine by pinging the RADIUS server from the device) — Take measures to make the device communicate with the RADIUS server normally.

Symptom 2: RADIUS packets cannot be sent to the RADIUS server.

Possible reasons and solutions:

- The communication links (physical/link layer) between the device and the RADIUS server is disconnected/blocked — Take measures to make the links connected/unblocked.
- None or incorrect RADIUS server IP address is set on the device — Be sure to set a correct RADIUS server IP address.
- One or all AAA UDP port settings are incorrect — Be sure to set the same UDP port numbers as those on the RADIUS server.

Symptom 3: The user passes the authentication and gets authorized, but the accounting information cannot be transmitted to the RADIUS server.

Possible reasons and solutions:

- The accounting port number is not properly set — Be sure to set a correct port number for RADIUS accounting.
- The device requests that both the authentication/authorization server and the accounting server use the same device (with the same IP address), but in fact they are not resident on the same device — Be sure to configure the RADIUS servers on the device according to the actual situation.

Troubleshooting HWTACACS Configuration

See the previous section if you encounter an HWTACACS fault.

3 EAD Configuration

Introduction to EAD

Endpoint admission defense (EAD) is an attack defense solution. Using this solution, you can enhance the active defense capability of network endpoints, prevents viruses and worms from spreading on the network, and protects the entire network by limiting the access rights of insecure endpoints.

With the cooperation of device, AAA sever, security policy server and security client, EAD is able to evaluate the security compliance of network endpoints and dynamically control their access rights.

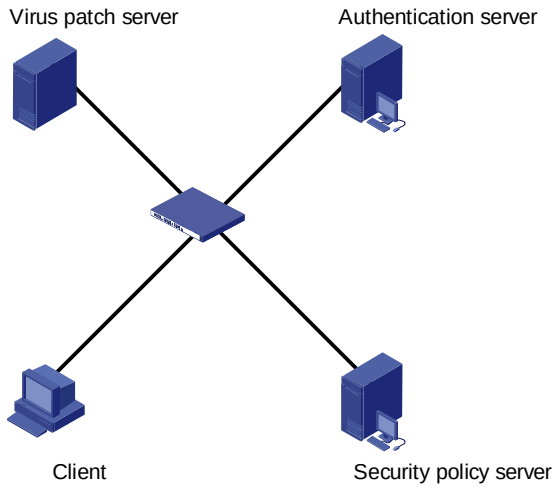
With EAD, a device:

- Verifies the validity of the session control packets it receives according to the source IP addresses of the packets: It regards only those packets sourced from authentication or security policy server as valid.
- Dynamically adjusts the VLAN, rate, packet scheduling priority and access control list (ACL) for user terminals according to session control packets, whereby to control the access rights of users dynamically.

Typical Network Application of EAD

EAD checks the security status of users before they can access the network, and forcibly implements user access control policies according to the check results. In this way, it can isolate the users that are not compliant with security standard and force these users to update their virus databases and install system patches. Figure 3-1 shows a typical network application of EAD.

Figure 3-1 Typical network application of EAD



After a client passes the authentication, the security Client (software installed on the client PC) interacts with the security policy server to check the security status of the client. If the client is not compliant with the security standard, the security policy server issues an ACL to the device, which then inhibits the client from accessing any parts of the network except for the virus/patch server.

After the client is patched and compliant with the required security standard, the security policy server reissues an ACL to the device, which then assigns access right to the client so that the client can access more network resources.

EAD Configuration

The EAD configuration includes:

- Configuring the attributes of access users (such as user name, user type, and password). For local authentication, you need to configure these attributes on the device; for remote authentication, you need to configure these attributes on the AAA sever.
- Configuring a RADIUS scheme.
- Configuring the IP address of the security policy server.
- Associating the ISP domain with the RADIUS scheme.

EAD is commonly used in RADIUS authentication environment.

This section mainly describes the configuration of security policy server IP address. For other related configuration, refer to AAA Overview.

Follow these steps to configure EAD:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter RADIUS scheme view	**radius scheme** *radius-scheme-name*	—
Configure the RADIUS server type to **extended**	**server-type extended**	Required
Configure the IP address of a security policy server	**security-policy-server** *ip-address*	Required Each RADIUS scheme supports up to eight IP addresses of security policy servers.

EAD Configuration Example

Network requirements

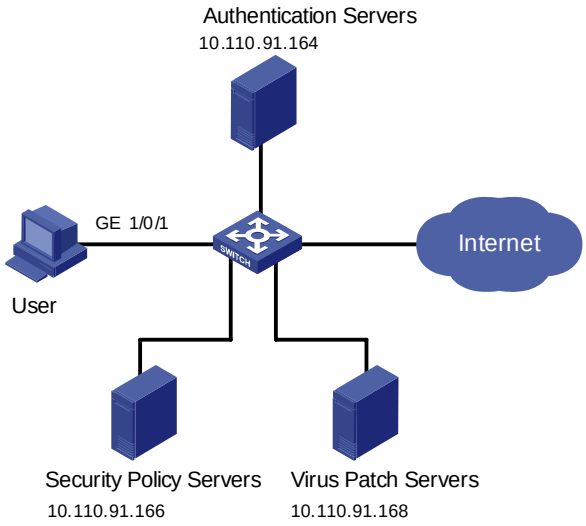
In Figure 3-2:

- A user is connected to GigabitEthernet 1/0/1 on the device.
- The user adopts iNode client supporting EAD extended function.
- You are required to configure the device to use RADIUS server for remote user authentication and use security policy server for EAD control on users.

The following are the configuration tasks:

- Connect the RADIUS authentication server 10.110.91.164 and the device, and configure the device to use port number 1812 to communicate with the server.
- Configure the authentication server type to **extended**.
- Configure the encryption password for exchanging messages between the device and RADIUS server to “expert”.
- Configure the IP address 10.110.91.166 of the security policy server.

Figure 3-2 EAD configuration



Configuration procedure

Configure 802.1x on the device. Refer to the section ”Configuring 802.1x” of *802.1x Configuration*.

Configure a domain.

```
<device> system-view
[device] domain system
[device-isp-system] quit
```

Configure a RADIUS scheme.

```
[device] radius scheme imc
[device-radius-imc] primary authentication 10.110.91.164 1812
[device-radius-imc] accounting optional
[device-radius-imc] key authentication expert
[device-radius-imc] server-type extended
```

Configure the IP address of the security policy server.

```
[device-radius-imc] security-policy-server 10.110.91.166
```

Associate the domain with the RADIUS scheme.

```
[device-radius-imc] quit
[device] domain system
[device-isp-system] radius-scheme imc
```

Table of Contents

1 MAC Authentication Configuration 1-1
MAC Authentication Overview 1-1
Performing MAC Authentication on a RADIUS Server 1-1
Performing MAC Authentication Locally 1-1
Related Concepts 1-2
MAC Authentication Timers 1-2
Quiet MAC Address 1-2
Configuring Basic MAC Authentication Functions 1-2
MAC Address Authentication Enhanced Function Configuration 1-4
MAC Address Authentication Enhanced Function Configuration Tasks 1-4
Configuring a Guest VLAN 1-4
Configuring the Maximum Number of MAC Address Authentication Users Allowed to Access a Port 1-6
Displaying and Maintaining MAC Authentication 1-7
MAC Authentication Configuration Example 1-7

1 MAC Authentication Configuration

Note

The sample output information in this manual was created on the WX3024. The output information on your device may vary.

MAC Authentication Overview

MAC authentication provides a way for authenticating users based on ports and MAC addresses, without requiring any client software to be installed on the hosts. Once detecting a new MAC address, it initiates the authentication process. During authentication, the user does not need to enter username or password manually.

The device implements MAC authentication locally or on a RADIUS server.

After determining the authentication method, users can select one of the following types of username as required:

- MAC address mode, where the MAC address of a user serves as both the username and the password.
- Fixed mode, where usernames and passwords are configured on the device in advance. In this case, the username, the password, and the limits on the total number of usernames are the matching criterion for successful authentication. For details, refer to *AAA* of this manual for information about local user attributes.

Performing MAC Authentication on a RADIUS Server

In RADIUS-based MAC authentication, the device serves as a RADIUS client and completes MAC authentication in combination of the RADIUS server.

- If the type of username is MAC address, the device sends a detected MAC address to the RADIUS server as both the username and password for authentication of the user.
- If the type of username is fixed username, the device sends the same username and password previously configured on the device to the RADIUS server for authentication of each user.

A user can access a network upon passing the authentication performed by the RADIUS server.

Performing MAC Authentication Locally

In local MAC authentication, the device performs authentication for users locally and different items need to be manually configured for users on the device according to the specified type of username:

- If the username type is MAC address, a local user must be configured for each user on the device, using the MAC address of the accessing user as the username. Hyphens must or must not be

included depending on the format configured with the **mac-authentication authmode usernameasmacaddress usernameformat** command; otherwise, the authentication will fail.

- If the username type is fixed username, you need to configure the fixed username and password on the device, which are used by the device to authenticate all users.

The service type of a local user needs to be configured as lan-access.

Related Concepts

MAC Authentication Timers

The following timers function in the process of MAC authentication:

- Offline detect timer: At this interval, the device checks to see whether an online user has gone offline. Once detecting that a user becomes offline, the device sends a stop-accounting notice to the RADIUS server.
- Quiet timer: Whenever a user fails MAC authentication, the device does not initiate any MAC authentication of the user during a period defined by this timer.
- Server timeout timer: During authentication of a user, if the device receives no response from the RADIUS server in this period, it assumes that its connection to the RADIUS server has timed out and forbids the user from accessing the network.

Quiet MAC Address

When a user fails MAC authentication, the MAC address becomes a quiet MAC address, which means that any packets from the MAC address will be discarded simply by the device until the quiet timer expires. This prevents an invalid user from being authenticated repeatedly in a short time.

 **Caution**

If the quiet MAC is the same as the static MAC configured or an authentication-passed MAC, then the quiet function is not effective.

Configuring Basic MAC Authentication Functions

Follow these steps to configure basic MAC authentication functions:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable MAC authentication globally	**mac-authentication**	Required Disabled by default

To do…	Use the command…		Remarks
Enable MAC authentication for the specified port(s) or the current port	In system view	**mac-authentication interface** *interface-list*	Use either method Disabled by default
	In interface view	**interface** *interface-type interface-number*	
		mac-authentication	
		quit	
Set the username in MAC address mode for MAC authentication	**mac-authentication authmode usernameasmacaddress** [**usernameformat** { **with-hyphen** | **without-hyphen** } { **lowercase** | **uppercase** } | **fixedpassword** *password*]		Optional By default, the MAC address of a user is used as the username.
Set the username in fixed mode for MAC authentication	Set the username in fixed mode for MAC authentication	**mac-authentication authmode usernamefixed**	Optional By default, the username is “mac” and no password is configured.
	Configure the username	**mac-authentication authusername** *username*	
	Configure the password	**mac-authentication authpassword** *password*	
Specify an ISP domain for MAC authentication	**mac-authentication domain** *isp-name*		Required The default ISP domain (default domain) is used by default.
Configure the MAC authentication timers	**mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }		Optional The default timeout values are as follows: 300 seconds for offline detect timer; 60 seconds for quiet timer; and 100 seconds for server timeout timer

Caution

- If MAC authentication is enabled on a port, you cannot configure the maximum number of dynamic MAC address entries for that port (through the **mac-address max-mac-count** command), and vice versa.
- If MAC authentication is enabled on a port, you cannot configure port security (through the **port-security enable** command) on that port, and vice versa.
- You can configure MAC authentication on a port before enabling it globally. However, the configuration will not take effect unless MAC authentication is enabled globally.

MAC Address Authentication Enhanced Function Configuration

MAC Address Authentication Enhanced Function Configuration Tasks

Complete the following tasks to configure MAC address authentication enhanced function:

Task	Remarks
Configuring a Guest VLAN	Optional
Configuring the Maximum Number of MAC Address Authentication Users Allowed to Access a Port	Optional

Configuring a Guest VLAN



Note

Different from Guest VLANs described in the *802.1x and System-Guard* manual, Guest VLANs mentioned in this section refer to Guests VLANs dedicated to MAC address authentication.

After completing configuration tasks in Configuring Basic MAC Authentication Functions for the device, the device can authenticate access users according to their MAC addresses or according to fixed usernames and passwords. The device will not learn MAC addresses of the clients failing in the authentication into its local MAC address table, thus prevent illegal users from accessing the network.

In some cases, if the clients failing in the authentication are required to access some restricted resources in the network (such as the virus library update server), you can use the Guest VLAN.

You can configure a Guest VLAN for each port of the device. When a client connected to a port fails in MAC address authentication, this port will be added into the Guest VLAN automatically. The MAC address of this client will also be learned into the MAC address table of the Guest VLAN, and thus the user can access the network resources of the Guest VLAN.

After a port is added to a Guest VLAN, the device will re-authenticate the first access user of this port (namely, the first user whose unicast MAC address is learned by the device) periodically. If this user passes the re-authentication, this port will exit the Guest VLAN, and thus the user can access the network normally.

Caution

- Guest VLANs are implemented in the mode of adding a port to a VLAN. For example, when multiple users are connected to a port, if the first user fails in the authentication, the other users can access only the contents of the Guest VLAN. The device will re-authenticate only the first user accessing this port, and the other users cannot be authenticated again. Thus, if more than one client is connected to a port, you cannot configure a Guest VLAN for this port.
- After users that are connected to an existing port failed to pass authentication, the device adds the port to the Guest VLAN. Therefore, the Guest VLAN can separate unauthenticated users on an access port. When it comes to a trunk port or a hybrid port, if a packet itself has a VLAN tag and be in the VLAN that the port allows to pass, the packet will be forwarded perfectly without the influence of the Guest VLAN. That is, packets can be forwarded to the VLANs other than the Guest VLAN through the trunk port and the hybrid port, even users fail to pass authentication.

Follow these steps to configure a Guest VLAN:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the Guest VLAN for the current port	**mac-authentication guest-vlan** *vlan-id*	Required By default, no Guest VLAN is configured for a port by default.
Return to system view	**quit**	—
Configure the interval at which the device re-authenticates users in Guest VLANs	**mac-authentication timer guest-vlan-reauth** *interval*	Optional By default, the device re-authenticates the users in Guest VLANs at the interval of 30 seconds by default.

Caution

- If more than one client is connected to a port, you cannot configure a Guest VLAN for this port.
- When a Guest VLAN is configured for a port, only one MAC address authentication user can access the port. Even if you set the limit on the number of MAC address authentication users to more than one, the configuration does not take effect.
- The undo vlan command cannot be used to remove the VLAN configured as a Guest VLAN. If you want to remove this VLAN, you must remove the Guest VLAN configuration for it. Refer to the VLAN module in this manual for the description on the undo vlan command.
- Only one Guest VLAN can be configured for a port, and the VLAN configured as the Guest VLAN must be an existing VLAN. Otherwise, the Guest VLAN configuration does not take effect. If you want to change the Guest VLAN for a port, you must remove the current Guest VLAN and then configure a new Guest VLAN for this port.
- 802.1x authentication cannot be enabled for a port configured with a Guest VLAN.
- The Guest VLAN function for MAC authentication does not take effect when port security is enabled.

Configuring the Maximum Number of MAC Address Authentication Users Allowed to Access a Port

You can configure the maximum number of MAC address authentication users for a port in order to control the maximum number of users accessing a port. After the number of access users has exceeded the configured maximum number, the device will not trigger MAC address authentication for subsequent access users, and thus these subsequent access users cannot access the network normally.

Follow these steps to configure the maximum number of MAC address authentication users allowed to access a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the maximum number of MAC address authentication users allowed to access a port	**mac-authentication max-auth-num** *user-number*	Required By default, the maximum number of MAC address authentication users allowed to access a port is 256.

Caution

- If both the limit on the number of MAC address authentication users and the limit on the number of users configured in the port security function are configured for a port, the smaller value of the two configured limits is adopted as the maximum number of MAC address authentication users allowed to access this port. Refer to the *Port Security manual* for the description on the port security function.
- You cannot configure the maximum number of MAC address authentication users for a port if any user connected to this port is online.

Displaying and Maintaining MAC Authentication

To do…	Use the command…	Remarks
Display global or on-port information about MAC authentication	**display mac-authentication** [**interface** *interface-list*]	Available in any view
Clear the statistics of global or on-port MAC authentication	**reset mac-authentication statistics** [**interface** *interface-type interface-number*]	Available in user view

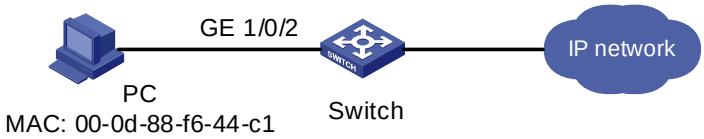
MAC Authentication Configuration Example

Network requirements

As illustrated in Figure 1-1, a supplicant is connected to Switch through port GigabitEthernet 1/0/2.

- MAC authentication is required on port GigabitEthernet 1/0/2 to control user access to the Internet.
- All users belong to domain aabbcc.net. The authentication is performed locally and the MAC address of the PC (00-0d-88-f6-44-c1) is used as both the username and password.

Figure 1-1 Network diagram for MAC authentication configuration



Configuration Procedure

Enable MAC authentication on port GigabitEthernet 1/0/2.

```
<device> system-view
[device] mac-authentication interface GigabitEthernet 1/0/2
```

Specify to use the user MAC address as both the username and password for MAC authentication, and specify the MAC address format as hyphened lowercase MAC address.

```
[device] mac-authentication authmode usernameasmacaddress usernameformat with-hyphen lowercase
```

Add a local user.

- Specify the username and password.

```
[device] local-user 00-0d-88-f6-44-c1
[device-luser-00-0d-88-f6-44-c1] password simple 00-0d-88-f6-44-c1
```

- Set the service type to “lan-access”.

```
[device-luser-00-0d-88-f6-44-c1] service-type lan-access
[device-luser-00-0d-88-f6-44-c1] quit
```

Add an ISP domain named aabbcc.net.

```
[device] domain aabbcc.net
New Domain added.
```

Specify to perform local authentication.

```
[device-isp-aabbcc.net] scheme local
[device-isp-aabbcc.net] quit
```

Specify aabbcc.net as the ISP domain for MAC authentication

```
[device] mac-authentication domain aabbcc.net
```

Enable MAC authentication globally (This is usually the last step in configuring access control related features. Otherwise, a user may be denied of access to the networks because of incomplete configuaration.)

```
[device] mac-authentication
```

After doing so, your MAC authentication configuration will take effect immediately. Only users with the MAC address of 00-0d-88-f6-44-c1 are allowed to access the Internet through port GigabitEthernet 1/0/2.

Table of Contents

1 IP Addressing Configuration 1-1
IP Addressing Overview 1-1
IP Address Classes 1-1
Special Case IP Addresses 1-2
Subnetting and Masking 1-2
Configuring IP Addresses 1-3
Displaying and Maintaining IP Addressing 1-4
IP Address Configuration Examples 1-4
IP Address Configuration Example I 1-4
IP Address Configuration Example II 1-5

2 IP Performance Configuration 2-1
IP Performance Overview 2-1
Introduction to IP Performance Configuration 2-1
Introduction to FIB 2-1
Configuring IP Performance 2-1
Configuration Task List 2-1
Configuring TCP Attributes 2-1
Disabling Sending of ICMP Error Packets 2-2
Displaying and Maintaining IP Performance Configuration 2-3

Note

- The term switch used throughout this document refers to a switching device in a generic sense or the switching engine of the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

1 IP Addressing Configuration

IP Addressing Overview

IP Address Classes

IP addressing uses a 32-bit address to identify each host on a network. An example is 01010000100000001000000010000000 in binary. To make IP addresses in 32-bit form easier to read, they are written in dotted decimal notation, each being four octets in length, for example, 10.1.1.1 for the address just mentioned.

Each IP address breaks down into two parts:

- Net ID: The first several bits of the IP address defining a network, also known as class bits.
- Host ID: Identifies a host on a network.

For administration sake, IP addresses are divided into five classes, as shown in the following figure (in which the blue parts represent the address class).

Figure 1-1 IP address classes

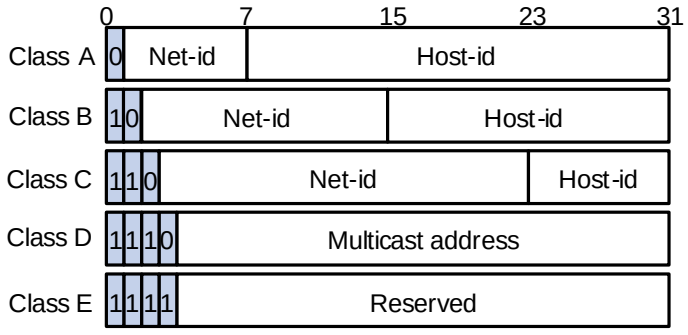


Table 1-1 describes the address ranges of these five classes. Currently, the first three classes of IP addresses are used in quantity.

Table 1-1 IP address classes and ranges

Class	Address range	Remarks
A	0.0.0.0 to 127.255.255.255	Address 0.0.0.0 means this host no this network. This address is used by a host at bootstrap when it does not know its IP address. This address is never a valid destination address. Addresses starting with 127 are reserved for loopback test. Packets destined to these addresses are processed locally as input packets rather than sent to the link.
B	128.0.0.0 to 191.255.255.255	—
C	192.0.0.0 to 223.255.255.255	—
D	224.0.0.0 to 239.255.255.255	Multicast address.
E	240.0.0.0 to 255.255.255.255	Reserved for future use except for the broadcast address 255.255.255.255.

Special Case IP Addresses

The following IP addresses are for special use, and they cannot be used as host IP addresses:

- IP address with an all-zeros net ID: Identifies a host on the local network. For example, IP address 0.0.0.16 indicates the host with a host ID of 16 on the local network.
- IP address with an all-zeros host ID: Identifies a network.
- IP address with an all-ones host ID: Identifies a directed broadcast address. For example, a packet with the destination address of 192.168.1.255 will be broadcasted to all the hosts on the network 192.168.1.0.

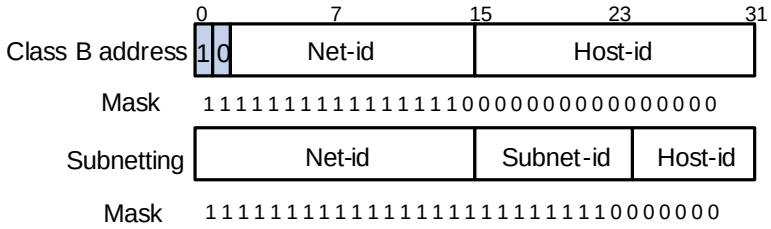
Subnetting and Masking

Subnetting was developed to address the risk of IP address exhaustion resulting from fast expansion of the Internet. The idea is to break a network down into smaller networks called subnets by using some bits of the host ID to create a subnet ID. To identify the boundary between the host ID and the combination of net ID and subnet ID, masking is used.

Each subnet mask comprises 32 bits related to the corresponding bits in an IP address. In a subnet mask, the part containing consecutive ones identifies the combination of net ID and subnet ID whereas the part containing consecutive zeros identifies the host ID.

Figure 1-2 shows how a Class B network is subnetted.

Figure 1-2 Subnet a Class B network



While allowing you to create multiple logical networks within a single Class A, B, or C network, subnetting is transparent to the rest of the Internet. All these networks still appear as one. As subnetting

adds an additional level, subnet ID, to the two-level hierarchy with IP addressing, IP routing now involves three steps: delivery to the site, delivery to the subnet, and delivery to the host.

In the absence of subnetting, some special addresses such as the addresses with the net ID of all zeros and the addresses with the host ID of all ones, are not assignable to hosts. The same is true of subnetting. When designing your network, you should note that subnetting is somewhat a tradeoff between subnets and accommodated hosts. For example, a Class B network can accommodate 65,534 (2^{16} – 2. Of the two deducted Class B addresses, one with an all-ones host ID is the broadcast address and the other with an all-zeros host ID is the network address) hosts before being subnetted. After you break it down into 512 (2^9) subnets by using the first 9 bits of the host ID for the subnet, you have only 7 bits for the host ID and thus have only 126 (2^7 – 2) hosts in each subnet. The maximum number of hosts is thus 64,512 (512 × 126), 1022 less after the network is subnetted.

Class A, B, and C networks, before being subnetted, use these default masks (also called natural masks): 255.0.0.0, 255.255.0.0, and 255.255.255.0 respectively.

Configuring IP Addresses

The device supports assigning IP addresses to VLAN interfaces and loopback interfaces. Besides directly assigning an IP address to a VLAN interface, you may configure a VLAN interface to obtain an IP address through BOOTP or DHCP as alternatives. If you change the way an interface obtains an IP address, from manual assignment to BOOTP for example, the IP address obtained from BOOTP will overwrite the old one manually assigned.

Note

This chapter only covers how to assign an IP address manually. For the other two approaches to IP address assignment, refer to the part discussing *DHCP* in this manual.

Follow these steps to assign an IP address to an interface:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Assign an IP address to the interface	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	Required No IP address is assigned by default.

Note

- You can assign at most two IP address to an interface, among which one is the primary IP address and another is secondary IP addresses. A newly specified primary IP address overwrites the previous one if there is any.
- The primary and secondary IP addresses of an interface cannot reside on the same network segment; the IP address of a VLAN interface must not be on the same network segment as that of a loopback interface on a device.
- A VLAN interface cannot be configured with a secondary IP address if the interface has been configured to obtain an IP address through BOOTP or DHCP.

Displaying and Maintaining IP Addressing

To do…	Use the command…	Remarks
Display information about a specified or all Layer 3 interfaces	**display ip interface** [*interface-type interface-number*]	Available in any view
Display brief configuration information about a specified or all Layer 3 interfaces	**display ip interface brief** [*interface-type* [*interface-number*]]	

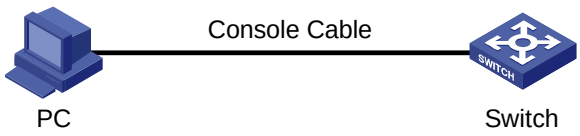
IP Address Configuration Examples

IP Address Configuration Example I

Network requirement

As shown in Figure 1-3, assign IP address 129.2.2.1 with mask 255.255.255.0 to VLAN-interface 1 of Switch.

Figure 1-3 Network diagram for IP address configuration



Configuration procedure

Configure an IP address for VLAN-interface 1.

```
<device> system-view
[device] interface vlan-interface 1
[device-Vlan-interface1] ip address 129.2.2.1 255.255.255.0
```

IP Address Configuration Example II

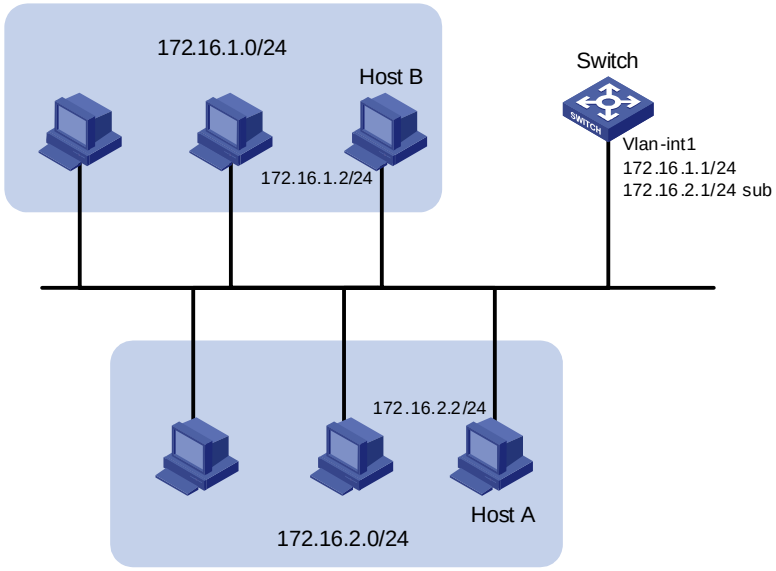
Network requirements

As shown in Figure 1-4, VLAN-interface 1 on Switch is connected to a LAN comprising two segments: 172.16.1.0/24 and 172.16.2.0/24.

To enable the hosts on the two network segments to communicate with the external network through Switch, and the hosts on the LAN can communicate with each other, do the following:

- Assign two IP addresses to VLAN-interface 1 on Switch.
- Set Switch as the gateway on all PCs of the two networks.

Figure 1-4 Network diagram for IP address configuration



Configuration procedure

Assign a primary IP address and a secondary IP address to VLAN-interface 1.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 172.16.1.1 255.255.255.0
[Switch-Vlan-interface1] ip address 172.16.2.1 255.255.255.0 sub
```

Set the gateway address to 172.16.1.1 on the PCs attached to the subnet 172.16.1.0/24, and to 172.16.2.1 on the PCs attached to the subnet 172.16.2.0/24.

Ping a host on the subnet 172.16.1.0/24 from Switch to check the connectivity.

```
<Switch> ping 172.16.1.2
  PING 172.16.1.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=255 time=25 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=255 time=27 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=255 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=255 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=255 time=26 ms

  --- 172.16.1.2 ping statistics ---
```

```
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/26/27 ms
```

The output information shows that Switch can communicate with the hosts on the subnet 172.16.1.0/24.

Ping a host on the subnet 172.16.2.0/24 from Switch to check the connectivity.

```
<Switch> ping 172.16.2.2
  PING 172.16.2.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=255 time=25 ms
    Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=255 time=26 ms

  --- 172.16.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/25/26 ms
```

The output information shows that Switch can communicate with the hosts on the subnet 172.16.2.0/24.

2 IP Performance Configuration

IP Performance Overview

Introduction to IP Performance Configuration

In some network environments, you need to adjust the IP parameters to achieve best network performance. The IP performance configuration supported by the device includes:

- Configuring TCP attributes
- Disabling sending of ICMP error packets

Introduction to FIB

Every device stores a forwarding information base (FIB). FIB is used to store the forwarding information of the device and guide Layer 3 packet forwarding.

You can know the forwarding information of the device through the FIB table. Each FIB entry includes: destination address/mask length, next hop, current flag, timestamp, and outbound interface.

When the device is running normally, the contents of the FIB and the routing table are the same.

Configuring IP Performance

Configuration Task List

Complete the following tasks to configure IP performance:

Task	Remarks
Configuring TCP Attributes	Optional
Disabling Sending of ICMP Error Packets	Optional

Configuring TCP Attributes

TCP optional parameters that can be configured include:

- synwait timer: When sending a SYN packet, TCP starts the synwait timer. If no response packets are received before the synwait timer times out, the TCP connection is not successfully created.
- finwait timer: When the TCP connection is changed into FIN_WAIT_2 state, finwait timer will be started. If no FIN packets are received within the timer timeout, the TCP connection will be terminated. If FIN packets are received, the TCP connection state changes to TIME_WAIT. If non-FIN packets are received, the system restarts the timer from receiving the last non-FIN packet. The connection is broken after the timer expires.
- Size of TCP receive/send buffer

Follow these steps to configure TCP attributes:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure TCP synwait timer's timeout value	**tcp timer syn-timeout** *time-value*	Optional By default, the timeout value is 75 seconds.
Configure TCP finwait timer's timeout value	**tcp timer fin-timeout** *time-value*	Optional By default, the timeout value is 675 seconds.
Configure the size of TCP receive/send buffer	**tcp window** *window-size*	Optional By default, the buffer is 8 kilobytes.

Disabling Sending of ICMP Error Packets

Sending error packets is a major function of ICMP protocol. In case of network abnormalities, ICMP packets are usually sent by the network or transport layer protocols to notify corresponding devices so as to facilitate control and management.

By default, the device supports sending ICMP redirect and destination unreachable packets.

Although sending ICMP error packets facilitate control and management, it still has the following disadvantages:

- Sending a lot of ICMP packets will increase network traffic.
- If receiving a lot of malicious packets that cause it to send ICMP error packets, the device's performance will be reduced.
- As the ICMP redirection function increases the routing table size of a host, the host's performance will be reduced if its routing table becomes very large.
- If a host sends malicious ICMP destination unreachable packets, end users may be affected.

To prevent the above mentioned problems, you can disable the device from sending such ICMP error packets.

Follow these steps to disable sending of ICMP error packets:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Disable sending of ICMP redirects	**undo icmp redirect send**	Required Enabled by default
Disable sending of ICMP destination unreachable packets	**undo icmp unreach send**	Required Enabled by default

Displaying and Maintaining IP Performance Configuration

To do…	Use the command…	Remarks
Display TCP connection status	**display tcp status**	Available in any view
Display TCP connection statistics	**display tcp statistics**	
Display UDP traffic statistics	**display udp statistics**	
Display IP traffic statistics	**display ip statistics**	
Display ICMP traffic statistics	**display icmp statistics**	
Display the current socket information of the system	**display ip socket** [**socktype** *sock-type*] [*task-id socket-id*]	
Display the forwarding information base (FIB) entries	**display fib**	
Display the FIB entries matching the destination IP address	**display fib** *ip_address1* [{ *mask1* | *mask-length1* } [*ip_address2* { *mask2* | *mask-length2* } | **longer**] | **longer**]	
Display the FIB entries permitted by a specific ACL	**display fib acl** *number*	
Display the FIB entries in the buffer which begin with, include or exclude the specified character string.	**display fib** | { **begin** | **include** | **exclude** } *regular-expression*	
Display the total number of the FIB entries	**display fib statistics**	
Clear IP traffic statistics	**reset ip statistics**	Available in user view
Clear TCP traffic statistics	**reset tcp statistics**	
Clear UDP traffic statistics	**reset udp statistics**	

Table of Contents

1 DHCP Overview 1-1
- Introduction to DHCP 1-1
- DHCP IP Address Assignment 1-1
  - IP Address Assignment Policy 1-1
  - Obtaining IP Addresses Dynamically 1-2
  - Updating IP Address Lease 1-3
- DHCP Packet Format 1-3
- Protocols and Standards 1-4

2 DHCP Relay Agent Configuration 2-1
- Introduction to DHCP Relay Agent 2-1
  - Usage of DHCP Relay Agent 2-1
  - DHCP Relay Agent Fundamentals 2-1
  - DHCP Relay Agent Support for Option 82 2-2
- Configuring the DHCP Relay Agent 2-4
  - DHCP Relay Agent Configuration Task List 2-4
  - Correlating a DHCP Server Group with a Relay Agent Interface 2-4
  - Configuring DHCP Relay Agent Security Functions 2-5
  - Configuring the DHCP Relay Agent to Support Option 82 2-7
- Displaying and Maintaining DHCP Relay Agent Configuration 2-8
- DHCP Relay Agent Configuration Example 2-8
- Troubleshooting DHCP Relay Agent Configuration 2-9

3 DHCP Snooping Configuration 3-1
- DHCP Snooping Overview 3-1
  - Function of DHCP Snooping 3-1
  - Overview of DHCP Snooping Option 82 3-2
  - Overview of IP Filtering 3-4
- DHCP Snooping Configuration 3-5
  - Configuring DHCP Snooping 3-5
  - Configuring DHCP Snooping to Support Option 82 3-6
  - Configuring IP Filtering 3-9
- DHCP Snooping Configuration Example 3-10
  - DHCP-Snooping Option 82 Support Configuration Example 3-10
  - IP Filtering Configuration Example 3-11
- Displaying and Maintaining DHCP Snooping Configuration 3-13

4 DHCP/BOOTP Client Configuration 4-1
- Introduction to DHCP Client 4-1
- Introduction to BOOTP Client 4-1
- Configuring a DHCP/BOOTP Client 4-1
- DHCP Client Configuration Example 4-2
- Displaying and Maintaining DHCP/BOOTP Client Configuration 4-3

Note

- The term switch used throughout this document refers to a switching device in a generic sense or the switching engine of the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

1 DHCP Overview

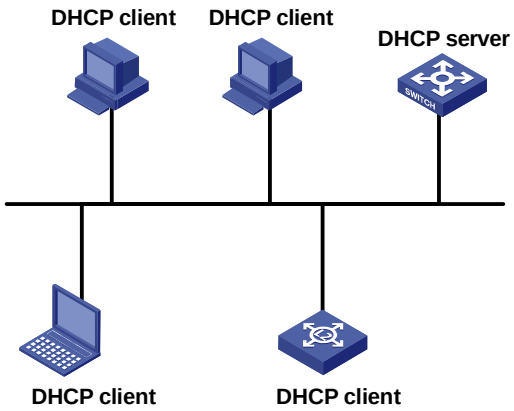
Introduction to DHCP

With networks getting larger in size and more complicated in structure, lack of available IP addresses becomes the common situation the network administrators have to face, and network configuration becomes a tough task for the network administrators. With the emerging of wireless networks and the using of laptops, the position change of hosts and frequent change of IP addresses also require new technology. Dynamic host configuration protocol (DHCP) is developed to solve these issues.

DHCP adopts a client/server model, where the DHCP clients send requests to DHCP servers for configuration parameters; and the DHCP servers return the corresponding configuration information such as IP addresses to implement dynamic allocation of network resources.

A typical DHCP application includes one DHCP server and multiple clients (such as PCs and laptops), as shown in Figure 1-1.

Figure 1-1 Typical DHCP application



DHCP IP Address Assignment

IP Address Assignment Policy

Currently, DHCP provides the following three IP address assignment policies to meet the requirements of different clients:

- Manual assignment. The administrator configures static IP-to-MAC bindings for some special clients, such as a WWW server. Then the DHCP server assigns these fixed IP addresses to the clients.
- Automatic assignment. The DHCP server assigns IP addresses to DHCP clients. The IP addresses will be occupied by the DHCP clients permanently.
- Dynamic assignment. The DHCP server assigns IP addresses to DHCP clients for predetermined period of time. In this case, a DHCP client must apply for an IP address again at the expiration of the period. This policy applies to most clients.

Obtaining IP Addresses Dynamically

A DHCP client undergoes the following four phases to dynamically obtain an IP address from a DHCP server:

1) Discover: In this phase, the DHCP client tries to find a DHCP server by broadcasting a DHCP-DISCOVER packet.
2) Offer: In this phase, the DHCP server offers an IP address. After the DHCP server receives the DHCP-DISCOVER packet from the DHCP client, it chooses an unassigned IP address from the address pool according to the priority order of IP address assignment and then sends the IP address and other configuration information together in a DHCP-OFFER packet to the DHCP client. The sending mode is decided by the flag filed in the DHCP-DISCOVER packet, refer to DHCP Packet Format for details.
3) Select: In this phase, the DHCP client selects an IP address. If more than one DHCP server sends DHCP-OFFER packets to the DHCP client, the DHCP client only accepts the DHCP-OFFER packet that first arrives, and then broadcasts a DHCP-REQUEST packet containing the assigned IP address carried in the DHCP-OFFER packet.
4) Acknowledge: In this phase, the DHCP servers acknowledge the IP address. Upon receiving the DHCP-REQUEST packet, only the selected DHCP server returns a DHCP-ACK packet to the DHCP client to confirm the assignment of the IP address to the client, or returns a DHCP-NAK packet to refuse the assignment of the IP address to the client. When the client receives the DHCP-ACK packet, it broadcasts an ARP packet with the assigned IP address as the destination address to detect the assigned IP address, and uses the IP address only if it does not receive any response within a specified period.

Note

- After the client receives the DHCP-ACK message, it will probe whether the IP address assigned by the server is in use by broadcasting a gratuitous ARP packet. If the client receives no response within specified time, the client can use this IP address. Otherwise, the client sends a DHCP-DECLINE message to the server and requests an IP address again.
- If there are multiple DHCP servers, IP addresses offered by other DHCP servers are assignable to other clients.

Updating IP Address Lease

After a DHCP server dynamically assigns an IP address to a DHCP client, the IP address keeps valid only within a specified lease time and will be reclaimed by the DHCP server when the lease expires. If the DHCP client wants to use the IP address for a longer time, it must update the IP lease.

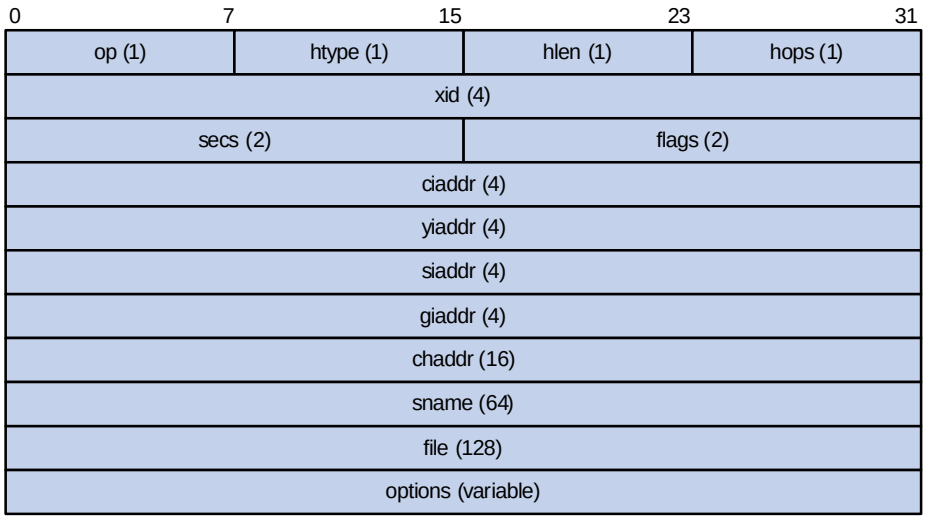
By default, a DHCP client updates its IP address lease automatically by unicasting a DHCP-REQUEST packet to the DHCP server when half of the lease time elapses. The DHCP server responds with a DHCP-ACK packet to notify the DHCP client of a new IP lease if the server can assign the same IP address to the client. Otherwise, the DHCP server responds with a DHCP-NAK packet to notify the DHCP client that the IP address will be reclaimed when the lease time expires.

If the DHCP client fails to update its IP address lease when half of the lease time elapses, it will update its IP address lease by broadcasting a DHCP-REQUEST packet to the DHCP servers again when seven-eighths of the lease time elapses. The DHCP server performs the same operations as those described above.

DHCP Packet Format

DHCP has eight types of packets. They have the same format, but the values of some fields in the packets are different. The DHCP packet format is based on that of the BOOTP packets. The following figure describes the packet format (the number in the brackets indicates the field length, in bytes):

Figure 1-2 DHCP packet format



The fields are described as follows:

- op: Operation types of DHCP packets, 1 for request packets and 2 for response packets.
- htype, hlen: Hardware address type and length of the DHCP client.
- hops: Number of DHCP relay agents which a DHCP packet passes. For each DHCP relay agent that the DHCP request packet passes, the field value increases by 1.
- xid: Random number that the client selects when it initiates a request. The number is used to identify an address-requesting process.
- secs: Elapsed time after the DHCP client initiates a DHCP request.
- flags: The first bit is the broadcast response flag bit, used to identify that the DHCP response packet is a unicast (set to 0) or broadcast (set to 1). Other bits are reserved.
- ciaddr: IP address of a DHCP client.
- yiaddr: IP address that the DHCP server assigns to a client.

- siaddr: IP address of the DHCP server.
- giaddr: IP address of the first DHCP relay agent that the DHCP client passes after it sent the request packet.
- chaddr: Hardware address of the DHCP client.
- sname: Name of the DHCP server.
- file: Path and name of the boot configuration file that the DHCP server specifies for the DHCP client.
- option: Optional variable-length fields, including packet type, valid lease time, IP address of a DNS server, and IP address of the WINS server.

Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol
- RFC 3046: DHCP Relay Agent Information option

2 DHCP Relay Agent Configuration

When configuring the DHCP relay agent, go to these sections for information you are interested in:

- Introduction to DHCP Relay Agent
- Configuring the DHCP Relay Agent
- Displaying and Maintaining DHCP Relay Agent Configuration
- DHCP Relay Agent Configuration Example
- Troubleshooting DHCP Relay Agent Configuration

Note

Currently, the interface-related DHCP relay agent configurations can only be made on VLAN interfaces.

Introduction to DHCP Relay Agent

Usage of DHCP Relay Agent

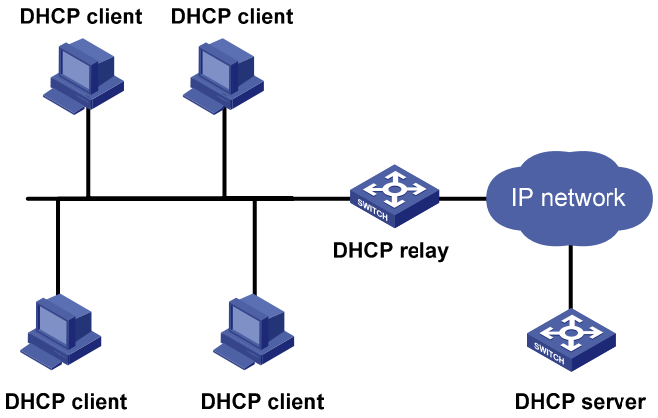
Since the packets are broadcasted in the process of obtaining IP addresses, DHCP is only applicable to the situation that DHCP clients and DHCP servers are in the same network segment, that is, you need to deploy at least one DHCP server for each network segment, which is far from economical.

DHCP relay agent is designed to address this problem. It enables DHCP clients in a subnet to communicate with the DHCP server in another subnet so that the DHCP clients can obtain IP addresses. In this case, the DHCP clients in multiple networks can use the same DHCP server, which can decrease your cost and provide a centralized administration.

DHCP Relay Agent Fundamentals

Figure 2-1 illustrates a typical DHCP relay agent application.

Figure 2-1 Typical DHCP relay agent application



In the process of dynamic IP address assignment through the DHCP relay agent, the DHCP client and DHCP server interoperate with each other in a similar way as they do without the DHCP relay agent. The following sections only describe the forwarding process of the DHCP relay agent. For the interaction process of the packets, see Obtaining IP Addresses Dynamically.

1) After receiving the DHCP-DISCOVER or DHCP-REQUEST broadcast from the client, the network device providing the DHCP relay agent function unicasts the message to the designated DHCP server based on the configuration.
2) The DHCP server selects an IP address and other parameters and sends the configuration information to the DHCP relay agent that relays the information to the client (the sending mode is decided by the flag filed in the client's DHCP-DISCOVER packet, refer to DHCP Packet Format for details).

DHCP Relay Agent Support for Option 82

Introduction to Option 82

Option 82 is the relay agent information option in the DHCP message. It records the location information of the DHCP client. With this option, the administrator can locate the DHCP client to further implement security control and accounting. The Option 82 supporting server can also use such information to define individual assignment policies of IP address and other parameters for the clients.

Option 82 involves at most 255 sub-options. If Option 82 is defined, at least one sub-option must be defined. Currently the DHCP relay agent supports two sub-options: sub-option 1 (circuit ID sub-option) and sub-option 2 (remote ID sub-option).

Padding content of Option 82

Option 82 has no unified definition in RFC 3046. Its padding information varies with vendors. Currently, the device that operates as a DHCP relay agent supports the extended padding format of Option 82 sub-options. By default, the sub-options of Option 82 are padded as follows, as shown in Figure 2-2 and Figure 2-3. (The content in brackets is the fixed value of each field.)

- Sub-option 1: Padded with the port index (smaller than the physical port number by 1) and VLAN ID of the port that received the client's request.
- Sub-option 2: Padded with the bridge MAC address of the DHCP relay agent device that received the client's request.

Figure 2-2 Padding contents for sub-option 1 of Option 82

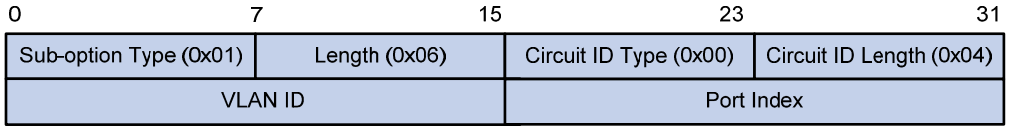
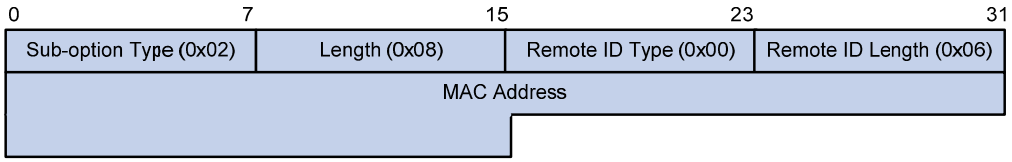


Figure 2-3 Padding contents for sub-option 2 of Option 82



Mechanism of Option 82 supported on DHCP relay agent

The procedure for a DHCP client to obtain an IP address from a DHCP server through a DHCP relay agent is similar to that for the client to obtain an IP address from a DHCP server directly. The following are the mechanism of Option 82 support on DHCP relay agent.

1) Upon receiving a DHCP request, the DHCP relay agent checks whether the packet contains Option 82 and processes the packet accordingly.

- If the request packet contains Option 82, the DHCP relay agent processes the packet depending on the configured strategy (that is, discards the packet, replaces the original Option 82 in the packet with its own, or leaves the original Option 82 unchanged in the packet), and forwards the packet (if not discarded) to the DHCP server.
- If the request packet does not contain Option 82, the DHCP relay agent adds Option 82 to the packet and forwards the packet to the DHCP server.

2) Upon receiving the packet returned from the DHCP server, the DHCP relay agent strips Option 82 from the packet and forwards the packet with the DHCP configuration information to the DHCP client.

Note

Request packets sent by a DHCP client fall into two categories: DHCP-DISCOVER packets and DHCP-REQUEST packets. As DHCP servers coming from different manufacturers process DHCP request packets in different ways (that is, some DHCP servers process Option 82 in DHCP-DISCOVER packets, whereas the rest process Option 82 in DHCP-REQUEST packets), a DHCP relay agent adds Option 82 to both types of packets to accommodate to DHCP servers of different manufacturers.

Configuring the DHCP Relay Agent

Note

If a device belongs to an IRF fabric, you need to enable the UDP Helper function on it before configuring it as a DHCP relay agent.

DHCP Relay Agent Configuration Task List

Complete the following tasks to configure the DHCP relay agent:

Task	Remarks
Correlating a DHCP Server Group with a Relay Agent Interface	Required
Configuring DHCP Relay Agent Security Functions	Optional
Configuring the DHCP Relay Agent to Support Option 82	Optional

Correlating a DHCP Server Group with a Relay Agent Interface

To enhance reliability, you can set multiple DHCP servers on the same network. These DHCP servers form a DHCP server group. When an interface of the relay agent establishes a correlation with the DHCP server group, the interface will forward received DHCP packets to all servers in the server group.

Follow these steps to correlate a DHCP server group with a relay agent interface:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the DHCP server IP address(es) in a specified DHCP server group	**dhcp-server** *groupNo* **ip** *ip-address*&<1-8>	Required By default, no DHCP server IP address is configured in a DHCP server group.
Map an interface to a DHCP server group	**interface** *interface-type interface-number*	Required By default, a VLAN interface is not mapped to any DHCP server group.
	dhcp-server *groupNo*	

Note

To improve security and avoid malicious attack to the unused SOCKETs, the device provides the following functions:

- UDP 67 and UDP 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP 67 and UDP 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows:

- When a VLAN interface is mapped to a DHCP server group with the **dhcp-server** command, the DHCP relay agent is enabled. At the same time, UDP 67 and UDP 68 ports used by DHCP are enabled.
- When the mapping between a VLAN interface and a DHCP server group is removed with the **undo dhcp-server** command, DHCP services are disabled. At the same time, UDP 67 and UDP 68 ports are disabled.

Note

- You can configure up to eight DHCP server IP addresses in a DHCP server group.
- You can map multiple VLAN interfaces to one DHCP server group. But one VLAN interface can be mapped to only one DHCP server group.
- If you execute the **dhcp-server groupNo** command repeatedly, the new configuration overwrites the previous one.
- You need to configure the group number specified in the **dhcp-server groupNo** command in VLAN interface view by using **dhcp-server groupNo ip ip-address&<1-8>** in advance.

Configuring DHCP Relay Agent Security Functions

Configuring address checking

After relaying an IP address from the DHCP server to a DHCP client, the DHCP relay agent can automatically record the client's IP-to-MAC binding and generate a dynamic address entry. It also supports static bindings, which means you can manually configure IP-to-MAC bindings on the DHCP relay agent, so that users can access external network using fixed IP addresses.

The purpose of the address checking function on DHCP relay agent is to prevent unauthorized users from statically configuring IP addresses to access external networks. With this function enabled, a DHCP relay agent inhibits a user from accessing external networks if the IP address configured on the user end and the MAC address of the user end do not match any entries (including the entries dynamically tracked by the DHCP relay agent and the manually configured static entries) in the user address table on the DHCP relay agent.

Follow these steps to configure address checking:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a static IP-to-MAC binding	**dhcp-security static** *ip-address mac-address*	Optional Not created by default.
Enter interface view	**interface** *interface-type interface-number*	—
Enable the address checking function	**address-check enable**	Required Disabled by default.

Note

- The **address-check enable** command is independent of other commands of the DHCP relay agent. That is, the invalid address check takes effect when this command is executed, regardless of whether other commands (such as the command to enable DHCP) are used.
- Before executing the **address-check enable** command on the interface connected to the DHCP server, you need to configure the static binding of the IP address to the MAC address of the DHCP server. Otherwise, the DHCP client will fail to obtain an IP address.

Configuring the dynamic client address entry updating function

After relaying an IP address from the DHCP server to the DHCP client, the DHCP relay agent can automatically record the client's IP-to-MAC binding and generate a dynamic address entry. But as a DHCP relay agent does not process DHCP-RELEASE packets, which are sent to DHCP servers by DHCP clients through unicast when the DHCP clients release IP addresses, the user address entries maintained by the DHCP cannot be updated in time. You can solve this problem by enabling the DHCP relay agent handshake function and configuring the dynamic client address entry updating interval.

After the handshake function is enabled, the DHCP relay agent sends the handshake packet (the DHCP-REQUEST packet) periodically to the DHCP server using a client's IP address and its own MAC address.

- If the DHCP relay agent receives the DHCP-ACK packet from the DHCP server, or receives no response from the server within a specified period, the IP address can be assigned. The DHCP relay agent ages out the corresponding entry in the client address table.
- If the DHCP relay agent receives the DHCP-NAK packet from the DHCP server, the lease of the IP address does not expire. The DHCP relay agent does not age out the corresponding entry.

Follow these steps to configure the dynamic user address entry updating function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the DHCP relay agent handshake function	**dhcp relay hand enable**	Optional Enabled by default.

To do…	Use the command…	Remarks
Set the interval at which the DHCP relay agent dynamically updates the client address entries	**dhcp-security tracker** { *interval* | **auto** }	Optional By default, **auto** is adopted, that is, the interval is automatically calculated.

Enabling unauthorized DHCP server detection

If there is an unauthorized DHCP server in the network, when a client applies for an IP address, the unauthorized DHCP server may assign an incorrect IP address to the DHCP client.

With this feature enabled, upon receiving a DHCP message with the siaddr field (IP addresses of the servers offering IP addresses to the client) not being 0 from a client, the DHCP relay agent will record the value of the siaddr field and the receiving interface. The administrator can use this information to check out any DHCP unauthorized servers.

Follow these steps to enable unauthorized DHCP server detection:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable unauthorized DHCP server detection	**dhcp-server detect**	Required Disabled by default.

Note

With the unauthorized DHCP server detection enabled, the relay agent will log all DHCP servers, including authorized ones, and each server is recorded only once until such information is removed and is recorded again. The administrator needs to find unauthorized DHCP servers from the system log information.

Configuring the DHCP Relay Agent to Support Option 82

Prerequisites

Before configuring Option 82 support on a DHCP relay agent, you need to:

- Configure network parameters and relay function of the DHCP relay device.
- Perform assignment strategy-related configurations, such as network parameters of the DHCP server, address pool, and lease time.
- The routes between the DHCP relay agent and the DHCP server are reachable.

Configuring the DHCP relay agent to support Option 82

Follow these steps to configure the DHCP relay agent to support Option 82:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable Option 82 support on the DHCP relay agent	**dhcp relay information enable**	Required Disabled by default.
Configure the strategy for the DHCP relay agent to process request packets containing Option 82	**dhcp relay information strategy** { **drop** | **keep** | **replace** }	Optional By default, the **replace** strategy is adopted

Note

- By default, with the Option 82 support function enabled on the DHCP relay agent, the DHCP relay agent will adopt the **replace** strategy to process the request packets containing Option 82. However, if other strategies are configured before, then enabling the 82 support on the DHCP relay agent will not change the configured strategies.
- To enable Option 82, you need to perform the corresponding configuration on the DHCP server and the DHCP relay agent.

Displaying and Maintaining DHCP Relay Agent Configuration

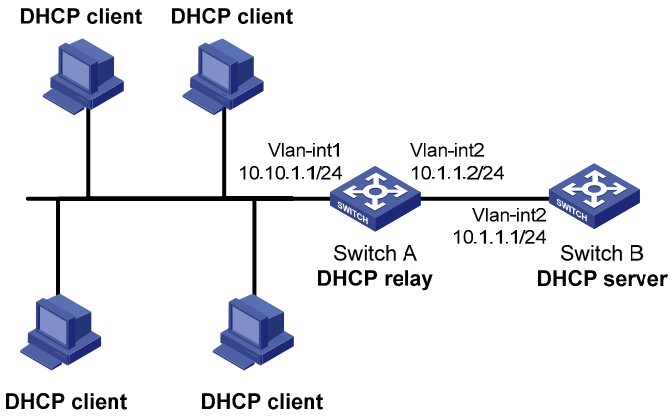
To do…	Use the command…	Remarks
Display the information about a specified DHCP server group	**display dhcp-server** *groupNo*	Available in any view
Display the information about the DHCP server group to which a specified VLAN interface is mapped	**display dhcp-server interface vlan-interface** *vlan-id*	
Display the specified client address entries on the DHCP relay agent	**display dhcp-security** [*ip-address* | **dynamic** | **static | tracker**]	
Clear the statistics information of the specified DHCP server group	**reset dhcp-server** *groupNo*	Available in user view

DHCP Relay Agent Configuration Example

Network requirements

As shown in Figure 2-4, VLAN-interface 1 on the DHCP relay agent (Switch A) connects to the network where DHCP clients reside. The IP address of VLAN-interface 1 is 10.10.1.1/24 and IP address of VLAN-interface 2 is 10.1.1.2/24 that communicates with the DHCP server 10.1.1.1/24. As shown in the figure below, Switch A forwards messages between DHCP clients and the DHCP server to assign IP addresses in subnet 10.10.1.0/24 to the clients.

Figure 2-4 Network diagram for DHCP relay agent



Configuration procedure

Create DHCP server group 1 and configure an IP address of 10.1.1.1 for it.

```
<SwitchA> system-view
[SwitchA] dhcp-server 1 ip 10.1.1.1
```

Map VLAN-interface 1 to DHCP server group 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] dhcp-server 1
```

Note

- You need to perform corresponding configurations on the DHCP server to enable the DHCP clients to obtain IP addresses from the DHCP server. The DHCP server configurations vary with different DHCP server devices, so the configurations are omitted.
- The DHCP relay agent and DHCP server must be reachable to each other.

Troubleshooting DHCP Relay Agent Configuration

Symptom

A client fails to obtain configuration information through a DHCP relay agent.

Analysis

This problem may be caused by improper DHCP relay agent configuration. When a DHCP relay agent operates improperly, you can locate the problem by enabling debugging and checking the information about debugging and interface state (You can display the information by executing the **corresponding display** command.)

Solution

- Check if DHCP is enabled on the DHCP server and the DHCP relay agent.

- Check if an address pool that is on the same network segment with the DHCP clients is configured on the DHCP server.
- Check if a reachable route is configured between the DHCP relay agent and the DHCP server.
- Check the DHCP relay agent. Check if the correct DHCP server group is configured on the interface connecting the network segment where the DHCP client resides. Check if the IP address of the DHCP server group is correct.
- If the **address-check enable** command is configured on the interface connected to the DHCP server, verify the DHCP server's IP-to-MAC address binding entry is configured on the DHCP relay agent; otherwise the DHCP client cannot obtain an IP address.

3 DHCP Snooping Configuration

Note

After DHCP snooping is enabled on a device, clients connected with the device cannot obtain IP addresses dynamically through BOOTP.

DHCP Snooping Overview

Function of DHCP Snooping

For security, the IP addresses used by online DHCP clients need to be tracked for the administrator to verify the corresponding relationship between the IP addresses the DHCP clients obtained from DHCP servers and the MAC addresses of the DHCP clients.

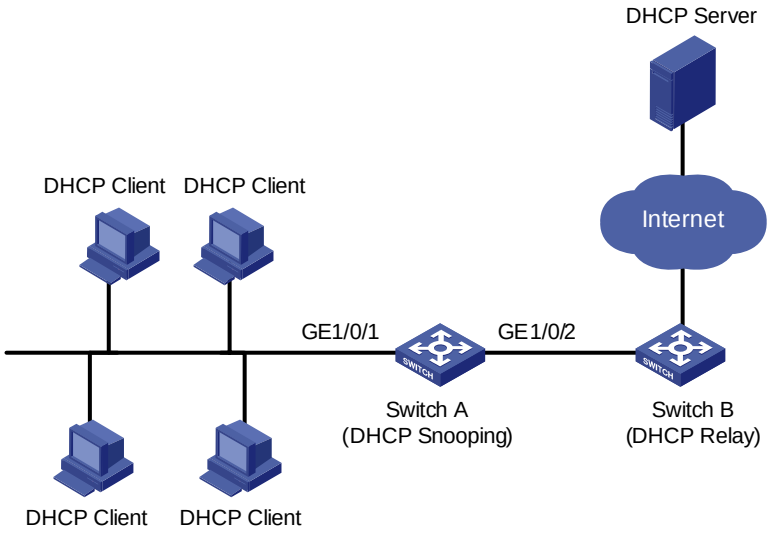
- Switches can track DHCP clients' IP addresses through the security function of the DHCP relay agent operating at the network layer.
- Switches can track DHCP clients' IP addresses through the DHCP snooping function at the data link layer.

When an unauthorized DHCP server exists in the network, a DHCP client may obtains an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, you can specify a port to be a trusted port or an untrusted port by the DHCP snooping function.

- Trusted: A trusted port is connected to an authorized DHCP server directly or indirectly. It forwards DHCP messages to guarantee that DHCP clients can obtain valid IP addresses.
- Untrusted: An untrusted port is connected to an unauthorized DHCP server. The DHCP-ACK or DHCP-OFFER packets received from the port are discarded, preventing DHCP clients from receiving invalid IP addresses.

Figure 3-1 illustrates a typical network diagram for DHCP snooping application, where Switch A is a WX3000 series device.

Figure 3-1 Typical network diagram for DHCP snooping application



DHCP snooping listens the following two types of packets to retrieve the IP addresses the DHCP clients obtain from DHCP servers and the MAC addresses of the DHCP clients:

- DHCP-REQUEST packet
- DHCP-ACK packet

Overview of DHCP Snooping Option 82

Introduction to Option 82

Option 82 is the relay agent information option in the DHCP message. It records the location information of the DHCP client.

When a DHCP relay agent (or a device enabled with DHCP snooping) receives a client's request, it adds the Option 82 to the request message and sends it to the server.

The administrator can locate the DHCP client to further implement security control and accounting. The Option 82 supporting server can also use such information to define individual assignment policies of IP address and other parameters for the clients.

Option 82 involves at most 255 sub-options. If Option 82 is defined, at least one sub-option must be defined. Currently the DHCP relay agent supports two sub-options: sub-option 1 (circuit ID sub-option) and sub-option 2 (remote ID sub-option).

Padding content and frame format of Option 82

There is no specification for what should be padded in Option 82. Manufacturers can pad it as required. By default, the sub-options of Option 82 for the device (enabled with DHCP snooping) are padded as follows:

- Sub-option 1 (circuit ID sub-option): Padded with the port index (smaller than the physical port number by 1) and VLAN ID of the port that received the client's request.
- Sub-option 2 (remote ID sub-option): Padded with the bridge MAC address of the DHCP snooping device that received the client's request.

By default, when the device serves as a DHCP snooping device, Option 82 adopts the extended format. Refer to Table 3-2 and Figure 3-3 for the extended format of the sub-options (with the default padding

contents). That is, the circuit ID or remote ID sub-option defines the type and length of a circuit ID or remote ID.

The remote ID type field and circuit ID type field are determined by the option storage format. They are both set to “0” in the case of HEX format and to “1” in the case of ASCII format.

Figure 3-2 Extended format of the circuit ID sub-option

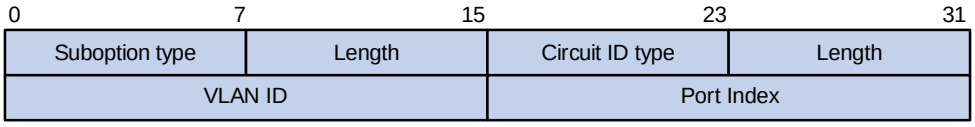
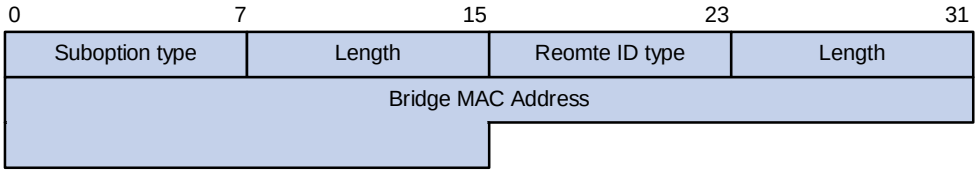


Figure 3-3 Extended format of the remote ID sub-option



In practice, some network devices do not support the type and length identifiers of the Circuit ID and Remote ID sub-options. To interwork with these devices, the device supports Option 82 in the standard format. Refer to Figure 3-4 and Figure 3-5 for the standard format of the sub-options (with the default padding contents). In the standard format, the Circuit ID or Remote ID sub-option does not contain the two-byte type and length fields of the circuit ID or remote ID.

Figure 3-4 Standard format of the circuit ID sub-option

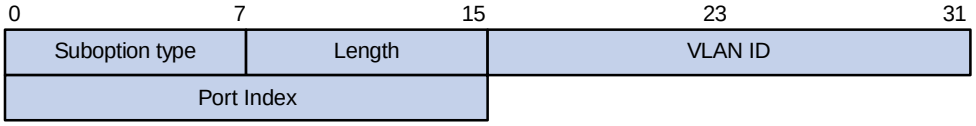
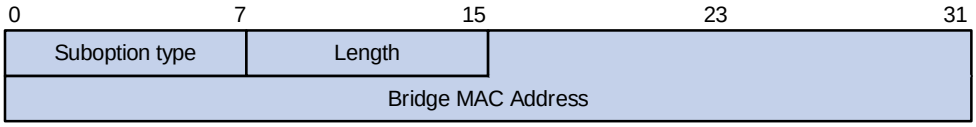


Figure 3-5 Standard format of the remote ID sub-option



Mechanism of DHCP-snooping Option 82

With DHCP snooping and DHCP-snooping Option 82 support enabled, when the DHCP snooping device receives a DHCP client’s request containing Option 82, it will handle the packet according to the handling policy and the configured contents in sub-options. For details, see Table 3-1.

Table 3-1 Ways of handling a DHCP packet with Option 82

Handling policy	Sub-option configuration	The DHCP snooping device will…
Drop	—	Drop the packet.
Keep	—	Forward the packet without changing Option 82.
Replace	Neither of the two sub-options is configured	Forward the packet after replacing the original Option 82 with the default content. The storage format of Option 82 content is the one specified with the **dhcp-snooping information format** command or the default HEX format if this command is not executed.
	Circuit ID sub-option is configured	Forward the packet after replacing the circuit ID sub-option of the original Option 82 with the configured circuit ID sub-option in ASCII format.
	Remote ID sub-option is configured	Forward the packet after replacing the remote ID sub-option of the original Option 82 with the configured remote ID sub-option in ASCII format.

When receiving a DHCP client's request without Option 82, the DHCP snooping device will add the option field with the configured sub-option and then forward the packet. For details, see Table 3-2.

Table 3-2 Ways of handling a DHCP packet without Option 82

Sub-option configuration	The DHCP snooping device will…
Neither of the two sub-options is configured.	Forward the packet after adding Option 82 with the default contents. The format of Option 82 is the one specified with the **dhcp-snooping information format** command or the default HEX format if this command is not executed.
Circuit ID sub-option is configured.	Forward the packet after adding Option 82 with the configured circuit ID sub-option in ASCII format.
Remote ID sub-option is configured.	Forward the packet after adding Option 82 with the configured remote ID sub-option in ASCII format.

Note

The circuit ID and remote ID sub-options in Option 82, which can be configured simultaneously or separately, are independent of each other in terms of configuration sequence.

When the DHCP snooping device receives a DHCP response packet from the DHCP server, the DHCP snooping device will delete the Option 82 field, if contained, before forwarding the packet, or will directly forward the packet if the packet does not contain the Option 82 field.

Overview of IP Filtering

A denial-of-service (DoS) attack means an attempt of an attacker sending a large number of forged address requests with different source IP addresses to the server so that the network cannot work normally. The specific effects are as follows:

- The resources on the server are exhausted, so the server does not respond to other requests.
- After receiving such type of packets, a device needs to send them to the CPU for processing. Too many request packets cause high CPU usage rate. As a result, the CPU cannot work normally.

The device can filter invalid IP packets through the DHCP-snooping table and IP static binding table.

DHCP-snooping table

After DHCP snooping is enabled on a device, a DHCP-snooping table is generated. It is used to record IP addresses obtained from the DHCP server, MAC addresses, the number of the port through which a client is connected to the DHCP-snooping-enabled device, and the number of the VLAN to which the port belongs to. These records are saved as entries in the DHCP-snooping table.

IP static binding table

The DHCP-snooping table only records information about clients that obtains IP address dynamically through DHCP. If a fixed IP address is configured for a client, the IP address and MAC address of the client cannot be recorded in the DHCP-snooping table. Consequently, this client cannot pass the IP filtering of the DHCP-snooping table, thus it cannot access external networks.

To solve this problem, the device supports the configuration of static binding table entries, that is, the binding relationship between IP address, MAC address, and the port connecting to the client, so that packets of the client can be correctly forwarded.

IP filtering

The device can filter IP packets in the following two modes:

- Filtering the source IP address in a packet. If the source IP address and the number of the port that receives the packet are consistent with entries in the DHCP-snooping table or static binding table, the device regards the packet as a valid packet and forwards it; otherwise, the device drops it directly.
- Filtering the source IP address and the source MAC address in a packet. If the source IP address and source MAC address in the packet, and the number of the port that receives the packet are consistent with entries in the DHCP-snooping table or static binding table, the device regards the packet as a valid packet and forwards it; otherwise, the device drops it directly.

DHCP Snooping Configuration

Configuring DHCP Snooping

Follow these steps to configure DHCP snooping:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable DHCP snooping	**dhcp-snooping**	Required By default, the DHCP snooping function is disabled.
Enter Ethernet port view	**interface** *interface-type interface-number*	—

To do…	Use the command…	Remarks
Specify the current port as a trusted port	**dhcp-snooping trust**	Required By default, after DHCP snooping is enabled, all ports of a device are untrusted ports.

Note

- You need to specify the ports connected to the valid DHCP servers as trusted to ensure that DHCP clients can obtain valid IP addresses. The trusted port and the port connected to the DHCP client must be in the same VLAN.
- You are not recommended to configure both the DHCP snooping and selective QinQ function on the device, which may result in the DHCP snooping to function abnormally.

Configuring DHCP Snooping to Support Option 82

Note

Enable DHCP snooping and specify trusted ports on the device before configuring DHCP snooping to support Option 82.

DHCP-Snooping Option 82 Support Configuration Task List

Complete the following tasks to configure DHCP-snooping Option 82 support:

Task	Remarks
Enable DHCP-snooping Option 82 support	Required
Configure a handling policy for DHCP packets with Option 82	Optional
Configure the storage format of Option 82	Optional
Configure the circuit ID sub-option	Optional
Configure the remote ID sub-option	Optional
Configure the padding format for Option 82	Optional

Enable DHCP-snooping Option 82 support

Follow these steps to enable DHCP-snooping Option 82 support:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable DHCP-snooping Option 82 support	**dhcp-snooping information enable**	Required By default, DHCP snooping Option 82 support is disabled.

Configure a handling policy for DHCP packets with Option 82

Follow these steps to configure a handling policy for DHCP packets with Option 82:

To do…	Use the command…	Remarks
Enter system view	**system-view**	Optional
Configure a global handling policy for requests that contain Option 82	**dhcp-snooping information strategy** { **drop** | **keep** | **replace** }	Optional The default handling policy is **replace**.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure a handling policy for requests that contain Option 82 received on the specified interface	**dhcp-snooping information strategy** { **drop** | **keep** | **replace** }	Optional The default policy is **replace**.

Note

If a handling policy is configured on a port, this configuration overrides the globally configured handling policy for requests received on this port, while the globally configured handling policy applies on those ports where a handling policy is not natively configured.

Configure the storage format of Option 82

The device supports the HEX or ASCII format for the Option 82 field.

Follow these steps to configure a storage format for the Option 82 field:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a storage format for the Option 82 field	**dhcp-snooping information format** { **hex | ascii** }	Optional By default, the format is **hex**.

Note

The **dhcp-snooping information format** command applies only to the default content of the Option 82 field. If you have configured the circuit ID or remote ID sub-option, the format of the sub-option is ASCII, instead of the one specified with the **dhcp-snooping information format** command.

Configure the circuit ID sub-option

Follow these steps to configure the circuit ID sub-option:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the circuit ID sub-option in Option 82	**dhcp-snooping information** [**vlan** *vlan-id*] **circuit-id string** *string*	Optional By default, the circuit ID sub-option contains the VLAN ID and port index related to the port that receives DHCP request packets from DHCP clients

Note

- In a port aggregation group, you can use this command to configure the primary and member ports respectively. When Option 82 is added, however, the circuit ID sub-option is subject to the one configured on the primary port.
- The circuit ID sub-option configured on a port will not be synchronized in the case of port aggregation.

Configure the remote ID sub-option

You can configure the remote ID sub-option in system view or Ethernet port view:

- In system view, the remote ID takes effect on all interfaces. You can configure Option 82 as the system name (sysname) of the device or any customized character string in the ASCII format.
- In Ethernet port view, the remote ID takes effect only on the current interface. You can configure Option 82 as any customized character string in the ASCII format for different VLANs. That is to say, you can add different configuration rules for packets from different VLANs.

Follow these steps to configure the remote ID sub-option in Option 82:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the remote ID sub-option in system view	**dhcp-snooping information remote-id** { **sysname | string** *string* }	Optional By default, the remote ID sub-option is the MAC address of the DHCP snooping device that received the DHCP client's request.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the remote ID sub-option in Ethernet port view	**dhcp-snooping information** [**vlan** *vlan-id*] **remote-id string** *string*	Optional By default, the remote ID sub-option is the MAC address of the DHCP snooping device that received the client's request.

Note

- If you configure a remote ID sub-option in both system view and on a port, the remote ID sub-option configured on the port applies when the port receives a packet, and the global remote ID applies to other interfaces that have no remote ID sub-option configured.
- In a port aggregation group, you can use this command to configure the primary and member ports respectively. When Option 82 is added, however, the remote ID is subject to the one configured on the primary port.
- The remote ID configured on a port will not be synchronized in the case of port aggregation.

Configure the padding format for Option 82

Follow these steps to configure the padding format for Option 82:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the padding format	**dhcp-snooping information packet-format** { **extended | standard** }	Optional By default, the padding format is in extended format.

Configuring IP Filtering

Follow these steps to configure IP filtering:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

To do…	Use the command…	Remarks
Enable IP filtering	**ip check source ip-address** [**mac-address**]	Required By default, this function is disabled.
Create an IP static binding entry	**ip source static binding ip-address** *ip-address* [**mac-address** *mac-address*]	Optional By default, no static binding entry is created.

Note

- Enable DHCP snooping and specify trusted ports on the device before configuring IP filtering.
- You are not recommended to configure IP filtering on the ports of an aggregation group.

DHCP Snooping Configuration Example

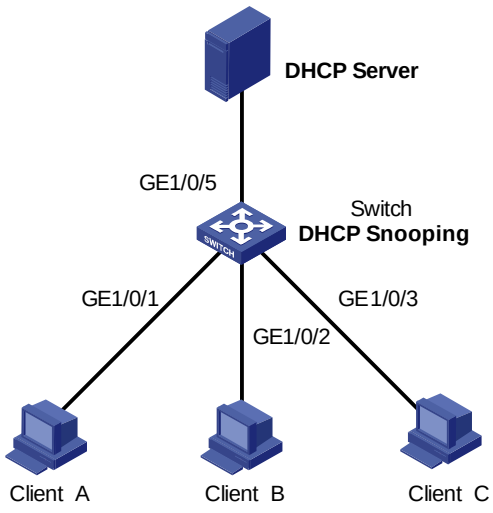
DHCP-Snooping Option 82 Support Configuration Example

Network requirements

As shown in Figure 3-6, GigabitEthernet 1/0/5 of Switch is connected to the DHCP server, and GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 are respectively connected to Client A, Client B, and Client C.

- Enable DHCP snooping on Switch.
- Specify GigabitEthernet 1/0/5 on Switch as a trusted port for DHCP snooping.
- Enable DHCP-snooping Option 82 support on Switch and set the remote ID field in Option 82 to the system name of Switch. Set the circuit ID sub-option to “abcd” in DHCP packets from VLAN 1 on GigabitEthernet 1/0/3.

Figure 3-6 Network diagram for DHCP-snooping Option 82 support configuration



Configuration procedure

Enable DHCP snooping on Switch.

```
<Switch> system-view
[Switch] dhcp-snooping
```

Specify GigabitEthernet 1/0/5 as the trusted port.

```
[Switch] interface gigabitethernet 1/0/5
[Switch-GigabitEthernet1/0/5] dhcp-snooping trust
[Switch-GigabitEthernet1/0/5] quit
```

Enable DHCP-snooping Option 82 support.

```
[Switch] dhcp-snooping information enable
```

Set the remote ID sub-option in Option 82 to the system name (sysname) of the DHCP snooping device.

```
[Switch] dhcp-snooping information remote-id sysname
```

Set the circuit ID sub-option in DHCP packets from VLAN 1 to “abcd” on GigabitEthernet 1/0/3.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] dhcp-snooping information vlan 1 circuit-id string abcd
```

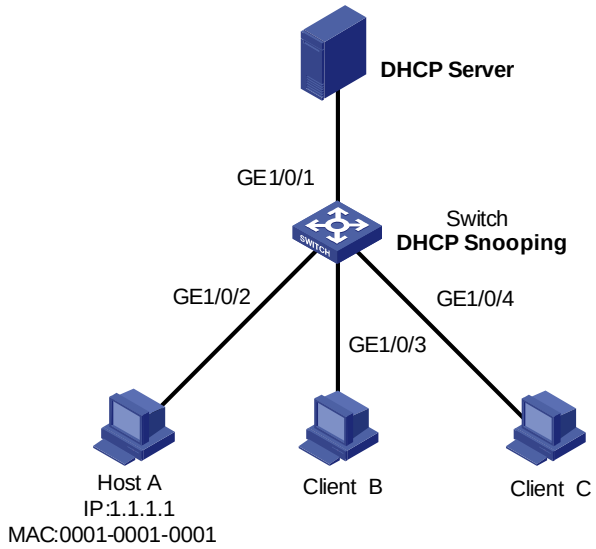
IP Filtering Configuration Example

Network requirements

As shown in Figure 3-7, GigabitEthernet 1/0/1 of Switch is connected to DHCP server and GigabitEthernet 1/0/2 is connected to Host A. The IP address and MAC address of Host A are 1.1.1.1 and 0001-0001-0001 respectively. GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 is connected to DHCP Client B and Client C.

- Enable DHCP snooping on Switch, and specify GigabitEthernet 1/0/1 as the DHCP snooping trusted port to prevent attacks from unauthorized DHCP servers.
- Enable IP filtering on GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to prevent attacks to the server from clients using fake source IP addresses.
- Create static binding entries on Switch, so that Host A using a fixed IP address can access the external network.

Figure 3-7 Network diagram for IP filtering configuration



Configuration procedure

Enable DHCP snooping on Switch.

```
<Switch> system-view
[Switch] dhcp-snooping
```

Specify GigabitEthernet 1/0/1 as the trusted port.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dhcp-snooping trust
[Switch-GigabitEthernet1/0/1] quit
```

Enable IP filtering on GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to filter packets based on the source IP addresses/MAC addresses.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] ip check source ip-address mac-address
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] ip check source ip-address mac-address
[Switch-GigabitEthernet1/0/3] quit
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] ip check source ip-address mac-address
[Switch-GigabitEthernet1/0/4] quit
```

Create static binding entries on GigabitEthernet 1/0/2 of Switch.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] ip source static binding ip-address 1.1.1.1 mac-address
0001-0001-0001
```

Displaying and Maintaining DHCP Snooping Configuration

To do…	Use the command…	Remarks
Display the user IP-MAC address mapping entries recorded by the DHCP snooping function	**display dhcp-snooping** [**unit** *unit-id*]	Available in any view
Display the (enabled/disabled) state of the DHCP snooping function and the trusted ports	**display dhcp-snooping trust**	
Display the IP static binding table	**display ip source static binding** [**vlan** *vlan-id* | **interface** *interface-type interface-number*]	

4 DHCP/BOOTP Client Configuration

Introduction to DHCP Client

After you specify a VLAN interface as a DHCP client, the device can use DHCP to obtain parameters such as IP address dynamically from the DHCP server, which facilitates user configuration and management.

Refer to Obtaining IP Addresses Dynamically for the process of how a DHCP client dynamically obtains an IP address through DHCP.

Introduction to BOOTP Client

After you specify an interface as a bootstrap protocol (BOOTP) client, the interface can use BOOTP to get information (such as IP address) from the BOOTP server, which simplifies your configuration.

Before using BOOTP, an administrator needs to configure a BOOTP parameter file for each BOOTP client on the BOOTP server. The parameter file contains information such as MAC address and IP address of a BOOTP client. When a BOOTP client sends a request to the BOOTP server, the BOOTP server will search for the BOOTP parameter file and return it to the client.

A BOOTP client dynamically obtains an IP address from a BOOTP server in the following way:

1) The BOOTP client broadcasts a BOOTP request, which contains its own MAC address.
2) The BOOTP server receives the request and searches for the corresponding IP address according to the MAC address of the BOOTP client and sends the information in a BOOTP response to the BOOTP client.
3) The BOOTP client obtains the IP address from the received response.

Note

Because a DHCP server can interact with a BOOTP client, you can use the DHCP server to assign an IP address to the BOOTP client, without needing to configure any BOOTP server.

Configuring a DHCP/BOOTP Client

Follow these steps to configure a DHCP/BOOTP client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface vlan-interface** *vlan-id*	—

To do…	Use the command…	Remarks
Configure the VLAN interface to obtain IP address through DHCP or BOOTP	**ip address** { **bootp-alloc** | **dhcp-alloc** }	Required By default, no IP address is configured for the VLAN interface.

Note

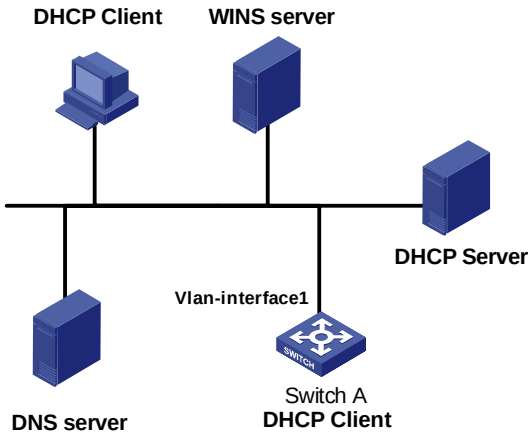
Currently, the device operating as a DHCP client can use an IP address for no more than 24 days; that is, it can obtain a lease with 24 days at most even if the DHCP server assigns a lease with more than 24 days.

DHCP Client Configuration Example

Network requirements

As shown in Figure 4-1, using DHCP, VLAN-interface 1 of Switch A is connected to the LAN to obtain an IP address from the DHCP server.

Figure 4-1 A DHCP network (Switch A serving as a DHCP client)



Configuration procedure

The following describes only the configuration on Switch A serving as a DHCP client.

Configure VLAN-interface 1 to dynamically obtain an IP address by using DHCP.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address dhcp-alloc
```

Displaying and Maintaining DHCP/BOOTP Client Configuration

To do…	Use the command…	Remarks
Display related information on a DHCP client	**display dhcp client** [**verbose**]	Available in any view
Display related information on a BOOTP client	**display bootp client** [**interface vlan-interface** *vlan-id*]	

Table of Contents

1 ACL Configuration 1-1
ACL Overview 1-1
ACL Matching Order 1-1
Ways to Apply an ACL on a Device 1-2
Types of ACLs Supported by Devices 1-3
ACL Configuration 1-3
Configuring Time Range 1-3
Configuring Basic ACL 1-5
Configuring Advanced ACL 1-6
Configuring Layer 2 ACL 1-7
ACL Assignment 1-8
Assigning an ACL Globally 1-9
Assigning an ACL to a VLAN 1-9
Assigning an ACL to a Port Group 1-10
Assigning an ACL to a Port 1-11
Displaying and Maintaining ACL 1-11
Examples for Upper-layer Software Referencing ACLs 1-12
Example for Controlling Telnet Login Users by Source IP 1-12
Example for Controlling Web Login Users by Source IP 1-12
Examples for Applying ACLs to Hardware 1-13
Basic ACL Configuration Example 1-13
Advanced ACL Configuration Example 1-13
Layer 2 ACL Configuration Example 1-14
Example for Applying an ACL to a VLAN 1-15

1 ACL Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a WX3000.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

ACL Overview

As the network scale and network traffic are increasingly growing, security control and bandwidth assignment play a more and more important role in network management. Filtering data packets can prevent a network from being accessed by unauthorized users efficiently while controlling network traffic and saving network resources. Access control lists (ACL) are often used to filter packets with configured matching rules.

Upon receiving a packet, the device compares the packet with the rules of the ACL applied on the current port to permit or discard the packet.

The rules of an ACL can be referenced by other functions that need traffic classification, such as QoS.

ACLs classify packets using a series of conditions known as rules. The conditions can be based on source addresses, destination addresses and port numbers carried in the packets.

According to their application purposes, ACLs fall into the following four types.

- Basic ACL. Rules are created based on source IP addresses only.
- Advanced ACL. Rules are created based on the Layer 3 and Layer 4 information such as the source and destination IP addresses, type of the protocols carried by IP, protocol-specific features, and so on.
- Layer 2 ACL. Rules are created based on the Layer 2 information such as source and destination MAC addresses, VLAN priorities, type of Layer 2 protocol, and so on.
- User-defined ACL. An ACL of this type matches packets by comparing the strings retrieved from the packets with specified strings. It defines the byte it begins to perform “and” operation with the mask on the basis of packet headers.

ACL Matching Order

An ACL can contain multiple rules, each of which matches specific type of packets. So the order in which the rules of an ACL are matched needs to be determined.

The rules in an ACL can be matched in one of the following two ways:

- **config**: where rules in an ACL are matched in the order defined by the user.

- **auto**: where rules in an ACL are matched in the order determined by the system, namely the “depth-first” rule.

For depth-first rule, there are two cases:

Depth-first match order for rules of a basic ACL

1) Range of source IP address: The smaller the source IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
2) Fragment keyword: A rule with the fragment keyword is prior to others.
3) If the above two conditions are identical, the earlier configured rule applies.

Depth-first match order for rules of an advanced ACL

1) Protocol range: A rule which has specified the types of the protocols carried by IP is prior to others.
2) Range of source IP address: The smaller the source IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
3) Range of destination IP address. The smaller the destination IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
4) Range of Layer 4 port number, that is, TCP/UDP port number. The smaller the range, the higher the match priority.
5) Number of parameters: the more the parameters, the higher the match priority.

If rule A and rule B are still the same after comparison in the above order, the weighting principles will be used in deciding their priority order. Each parameter is given a fixed weighting value. This weighting value and the value of the parameter itself will jointly decide the final matching order. Involved parameters with weighting values from high to low are **icmp-type**, **established**, **dscp**, **tos**, **precedence**, **fragment**. Comparison rules are listed below.

- The smaller the weighting value left, which is a fixed weighting value minus the weighting value of every parameter of the rule, the higher the match priority.
- If the types of parameter are the same for multiple rules, then the sum of parameters’ weighting values of a rule determines its priority. The smaller the sum, the higher the match priority.

Ways to Apply an ACL on a Device

Being applied to the hardware directly

In the device, an ACL can be directly applied to hardware for packet filtering and traffic classification. In this case, the rules in an ACL are matched in the order determined by the hardware instead of that defined in the ACL. For devices, the earlier the rule applies, the higher the match priority.

ACLs are directly applied to hardware when they are used for:

- Implementing QoS
- Filtering the packets to be forwarded

Being referenced by upper-level software

ACLs can also be used to filter and classify the packets to be processed by software. In this case, the rules in an ACL can be matched in one of the following two ways:

- **config**, where rules in an ACL are matched in the order defined by the user.
- **auto**, where the rules in an ACL are matched in the order determined by the system, namely the “depth-first” order.

When applying an ACL in this way, you can specify the order in which the rules in the ACL are matched. The match order cannot be modified once it is determined, unless you delete all the rules in the ACL and define the match order.

An ACL can be referenced by upper-layer software:

- Referenced by routing policies
- Used to control Telnet, SNMP and Web login users

 **Note**

- When an ACL is directly applied to hardware for packet filtering, the device will permit packets if the packets do not match the ACL.
- When an ACL is referenced by upper-layer software to control Telnet, SNMP and Web login users, the device will deny packets if the packets do not match the ACL.

Types of ACLs Supported by Devices

The devices support the following types of ACLs.

- Basic ACLs
- Advanced ACLs
- Layer 2 ACLs

ACLs defined on the devices can be applied to hardware directly or referenced by upper-layer software for packet filtering.

ACL Configuration

Configuring Time Range

Time ranges can be used to filter packets. You can specify a time range for each rule in an ACL. A time range-based ACL takes effect only in specified time ranges. Only after a time range is configured and the system time is within the time range, can an ACL rule take effect.

Two types of time ranges are available:

- Periodic time range, which recurs periodically on the day or days of the week.
- Absolute time range, which takes effect only in a period of time and does not recur.

 **Note**

An absolute time range on a device can be within the range 1970/1/1 00:00 to 2100/12/31 24:00.

Configuration Procedure

Follow these steps to configure a time range:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a time range	**time-range** *time-name* { *start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date* }	Required

Note that:

- If only a periodic time section is defined in a time range, the time range is active only when the system time is within the defined periodic time section. If multiple periodic time sections are defined in a time range, the time range is active only when the system time is within one of the periodic time sections.
- If only an absolute time section is defined in a time range, the time range is active only when the system time is within the defined absolute time section. If multiple absolute time sections are defined in a time range, the time range is active only when the system time is within one of the absolute time sections.
- If both a periodic time section and an absolute time section are defined in a time range, the time range is active only when the periodic time range and the absolute time range are both matched. Assume that a time range contains an absolute time section ranging from 00:00 January 1, 2004 to 23:59 December 31, 2004, and a periodic time section ranging from 12:00 to 14:00 on every Wednesday. This time range is active only when the system time is within the range from 12:00 to 14:00 on every Wednesday in 2004.
- If the start time is not specified, the time section starts from 1970/1/1 00:00 and ends on the specified end date. If the end date is not specified, the time section starts from the specified start date to 2100/12/31 23:59.

Configuration Example

Define a periodic time range that spans from 8:00 to 18:00 on Monday through Friday.

```
<device> system-view
[device] time-range test 8:00 to 18:00 working-day
[device] display time-range test
Current time is 13:27:32 Apr/16/2005 Saturday

Time-range : test ( Inactive )
 08:00 to 18:00 working-day
```

Define an absolute time range spans from 15:00 1/28/2006 to 15:00 1/28/2008.

```
<device> system-view
[device] time-range test from 15:00 1/28/2006 to 15:00 1/28/2008
[device] display time-range test
Current time is 13:30:32 Apr/16/2005 Saturday

Time-range : test ( Inactive )
 From 15:00 Jan/28/2000 to 15:00 Jan/28/2004
```

Configuring Basic ACL

A basic ACL filters packets based on their source IP addresses.

A basic ACL can be numbered from 2000 to 2999.

Configuration Prerequisites

- To configure a time range-based basic ACL rule, you need to create the corresponding time range first. For information about time range configuration, refer to Configuring Time Range.
- The source IP addresses based on which the ACL filters packets are determined.

Configuration Procedure

Follow these steps to define a basic ACL rule:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create an ACL and enter basic ACL view	**acl number** *acl-number* [**match-order** { **auto** | **config** }]	Required **config** by default
Define an ACL rule	**rule** [*rule-id*] { **deny** | **permit** } [*rule-string*]	Required For information about *rule-string*, refer to *ACL Command*.
Configure a description string to the ACL	**description** *text*	Optional Not configured by default

Note that:

- With the **config** match order specified for the basic ACL, you can modify any existent rule. The unmodified part of the rule remains. With the **auto** match order specified for the basic ACL, you cannot modify any existent rule; otherwise the system prompts error information.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, it is the maximum rule number plus one.
- The content of a modified or created rule cannot be identical with the content of any existing rule; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.
- With the **auto** match order specified, the newly created rules will be inserted in the existent ones by depth-first principle, but the numbers of the existent rules are unaltered.

Configuration Example

Configure ACL 2000 to deny packets whose source IP addresses are 192.168.0.1.

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule deny source 192.168.0.1 0
```

Display the configuration information of ACL 2000.

```
[device-acl-basic-2000] display acl 2000
Basic ACL  2000, 1 rule
Acl's step is 1
```

```
rule 0 deny source 192.168.0.1 0
```

Configuring Advanced ACL

An advanced ACL can filter packets by their source and destination IP addresses, the protocols carried by IP, and protocol-specific features such as TCP/UDP source and destination ports, ICMP message type and message code.

An advanced ACL can be numbered from 3000 to 3999. Note that ACL 3998 and ACL 3999 cannot be configured because they are reserved for cluster management.

Advanced ACLs support analysis and processing of three packet priority levels: type of service (ToS) priority, IP priority and differentiated services codepoint (DSCP) priority.

Using advanced ACLs, you can define classification rules that are more accurate, more abundant, and more flexible than those defined for basic ACLs.

Configuration Prerequisites

- To configure a time range-based advanced ACL rule, you need to create the corresponding time ranges first. For information about of time range configuration, refer to Configuring Time Range.
- The settings to be specified in the rule, such as source and destination IP addresses, the protocols carried by IP, and protocol-specific features, are determined.

Configuration Procedure

Follow these steps to define an advanced ACL rule:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create an advanced ACL and enter advanced ACL view	**acl number** *acl-number* [**match-order** { **auto** | **config** }]	Required **config** by default
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } *protocol* [*rule-string*]	Required For information about *protocol* and *rule-string*, refer to *ACL Command*.
Assign a description string to the ACL rule	**rule** *rule-id* **comment** *text*	Optional No description by default
Assign a description string to the ACL	**description** *text*	Optional No description by default

Note that:

- With the **config** match order specified for the advanced ACL, you can modify any existent rule. The unmodified part of the rule remains. With the **auto** match order specified for the ACL, you cannot modify any existent rule; otherwise the system prompts error information.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, it is the maximum rule number plus one.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.

- If the ACL is created with the **auto** keyword specified, the newly created rules will be inserted in the existent ones by depth-first principle, but the numbers of the existent rules are unaltered.

Configuration Example

Configure ACL 3000 to permit the TCP packets sourced from the network 129.9.0.0/16 and destined for the network 202.38.160.0/24 and with the destination port number being 80.

```
<device> system-view
[device] acl number 3000
[device-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0
0.0.0.255 destination-port eq 80
```

Display the configuration information of ACL 3000.

```
[device-acl-adv-3000] display acl 3000
Advanced ACL  3000, 1 rule
Acl's step is 1
 rule  0  permit  tcp  source  129.9.0.0  0.0.255.255  destination  202.38.160.0  0.0.0.255
destination-port eq www
```

Configuring Layer 2 ACL

Layer 2 ACLs filter packets according to their Layer 2 information, such as the source and destination MAC addresses, VLAN priority, and Layer 2 protocol types.

A Layer 2 ACL can be numbered from 4000 to 4999.

Configuration Prerequisites

- To configure a time range-based Layer 2 ACL rule, you need to create the corresponding time ranges first. For information about time range configuration, refer to Configuring Time Range.
- The settings to be specified in the rule, such as source and destination MAC addresses, VLAN priorities, and Layer 2 protocol types, are determined.

Configuration Procedure

Follow these steps to define a Layer 2 ACL rule:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a Layer 2 ACL and enter layer 2 ACL view	**acl number** *acl-number*	Required
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	Required For information about *rule-string*, refer to *ACL Command*.
Assign a description string to the ACL rule	**rule** *rule-id* **comment** *text*	Optional No description by default
Assign a description string to the ACL	**description** *text*	Optional No description by default

Note that:

- You can modify any existent rule of the Layer 2 ACL and the unmodified part of the ACL remains.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, it is the maximum rule number plus one.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.

Configuration Example

Configure ACL 4000 to deny packets sourced from the MAC address 000d-88f5-97ed, destined for the MAC address 0011-4301-991e, and with their 802.1p priority being 3.

```
<device> system-view
[device] acl number 4000
[device-acl-ethernetframe-4000] rule deny cos 3 source 000d-88f5-97ed ffff-ffff-ffff dest
0011-4301-991e ffff-ffff-ffff
```

Display the configuration information of ACL 4000.

```
[device-acl-ethernetframe-4000] display acl 4000
Ethernet frame ACL  4000, 1 rule
Acl's step is 1
 rule 0 deny cos excellent-effort source 000d-88f5-97ed ffff-ffff-ffff dest 0011-4301-991e
ffff-ffff-ffff
```

ACL Assignment

On a device, you can assign ACLs to the hardware for packet filtering.

As for ACL assignment, the following four ways are available.

- Assigning ACLs globally, for filtering the inbound packets on all the ports.
- Assigning ACLs to a VLAN, for filtering the inbound packets on all the ports and belonging to a VLAN.
- Assigning ACLs to a port group, for filtering the inbound packets on all the ports in a port group. For information about port group, refer to *Basic Port Operation*.
- Assigning ACLs to a port, for filtering the inbound packets on a port.

You can assign ACLs in the above-mentioned ways as required.

Caution

- ACLs assigned globally take precedence over those that are assigned to VLANs. That is, when a packet matches a rule of a globally assigned ACL and a rule of an ACL assigned to a VLAN, the device will perform the action defined in the rule of the globally assigned ACL if the actions defined in the two rules conflict.
- When a packet matches a rule of an ACL assigned globally (or assigned to a VLAN) and a rule of an ACL assigned to a port (or port group), the device will deny the packets if the actions defined in the two rules conflict.
- ACLs assigned globally or to a VLAN take precedence over the default ACL. However, assigning ACLs globally or to a VLAN may affect device management that is implemented through Telnet and so on.

Assigning an ACL Globally

Configuration prerequisites

Before applying ACL rules to a VLAN, you need to define the related ACLs. For information about defining an ACL, refer to Configuring Basic ACL, Configuring Advanced ACL, Configuring Layer 2 ACL.

Configure procedure

Follow these steps to assign an ACL globally:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Assign an ACL globally	**packet-filter inbound** *acl-rule*	Required For description on the *acl-rule* argument, refer to *ACL Command*.

Configuration example

Apply ACL 2000 globally to filter the inbound packets on all the ports.

```
<device> system-view
[device] packet-filter inbound ip-group 2000
```

Assigning an ACL to a VLAN

Configuration prerequisites

Before applying ACL rules to a VLAN, you need to define the related ACLs. For information about defining an ACL, refer to Configuring Basic ACL, Configuring Advanced ACL, Configuring Layer 2 ACL.

Configuration procedure

Follow these steps to assign an ACL to a VLAN:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Apply an ACL to a VLAN	**packet-filter vlan** *vlan-id* **inbound** *acl-rule*	Required For description on the *acl-rule* argument, refer to *ACL Command*.

Configuration example

Apply ACL 2000 to VLAN 10 to filter the inbound packets of VLAN 10 on all the ports.

```
<device> system-view
[device] packet-filter vlan 10 inbound ip-group 2000
```

Assigning an ACL to a Port Group

Configuration prerequisites

Before applying ACL rules to a VLAN, you need to define the related ACLs. For information about defining an ACL, refer to Configuring Basic ACL, Configuring Advanced ACL, Configuring Layer 2 ACL.

Configuration procedure

Follow these steps to assign an ACL to a port group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter port group view	**port-group** *group-id*	—
Apply an ACL to the port group	**packet-filter inbound** *acl-rule*	Required For description on the *acl-rule* argument, refer to *ACL Command*.

Note

After an ACL is assigned to a port group, it will be automatically assigned to the ports that are subsequently added to the port group.

Configuration example

Apply ACL 2000 to port group 1 to filter the inbound packets on all the ports in the port group.

```
<device> system-view
[device] port-group 1
[device-port-group-1] packet-filter inbound ip-group 2000
```

Assigning an ACL to a Port

Configuration prerequisites

Before applying ACL rules to a VLAN, you need to define the related ACLs. For information about defining an ACL, refer to Configuring Basic ACL, Configuring Advanced ACL, Configuring Layer 2 ACL.

Configuration procedure

Follow these steps to apply an ACL to a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Apply an ACL to the port	**packet-filter inbound** *acl-rule*	Required For description on the *acl-rule* argument, refer to *ACL Command*.

Note

You cannot assign an ACL to a member port of a port group.

Configuration example

Apply ACL 2000 to GigabitEthernet 1/0/1 to filter the inbound packets.

```
<device> system-view
[device] interface GigabitEthernet 1/0/1
[device-GigabitEthernet1/0/1] packet-filter inbound ip-group 2000
```

Displaying and Maintaining ACL

To do…	Use the command…	Remarks
Display a configured ACL or all the ACLs	**display acl** { **all** | *acl-number* }	Available in any view.
Display a time range or all the time ranges	**display time-range** { **all** | *time-name* }	
Display the information about packet filtering	**display packet-filter** { **global | interface** *interface-type interface-number* | **port-group** [*group-id*] | **unitid** *unit-id* **| vlan** [*vlan-id*] }	
Display information about remaining ACL resources	**display acl remaining entry**	

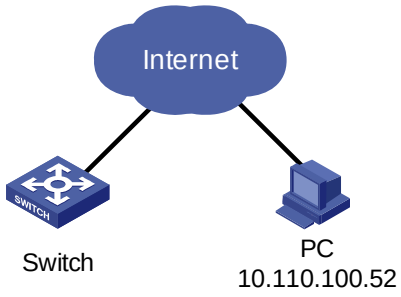
Examples for Upper-layer Software Referencing ACLs

Example for Controlling Telnet Login Users by Source IP

Network requirements

As shown in Figure 1-1, apply an ACL to permit users with the source IP address of 10.110.100.52 to telnet to the switching engine.

Figure 1-1 Network diagram for controlling Telnet login users by source IP



Configuration procedure

Define ACL 2000.

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[device-acl-basic-2000] quit
```

Reference ACL 2000 on VTY user interface to control Telnet login users.

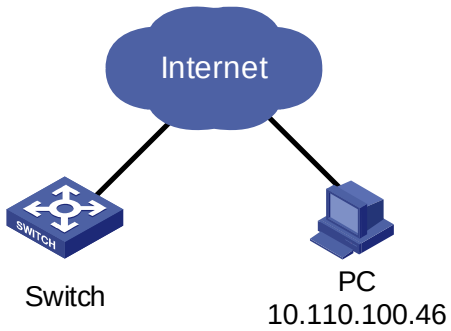
```
[device] user-interface vty 0 4
[device-ui-vty0-4] acl 2000 inbound
```

Example for Controlling Web Login Users by Source IP

Network requirements

As shown in Figure 1-2, apply an ACL to permit Web users with the source IP address of 10.110.100.46 to log in to the Switch through HTTP.

Figure 1-2 Network diagram for controlling Web login users by source IP



Configuration procedure

Define ACL 2001.

```
<device> system-view
[device] acl number 2001
[device-acl-basic-2001] rule 1 permit source 10.110.100.46 0
[device-acl-basic-2001] quit
```

Reference ACL 2001 to control users logging in to the Web server.

```
[device] ip http acl 2001
```

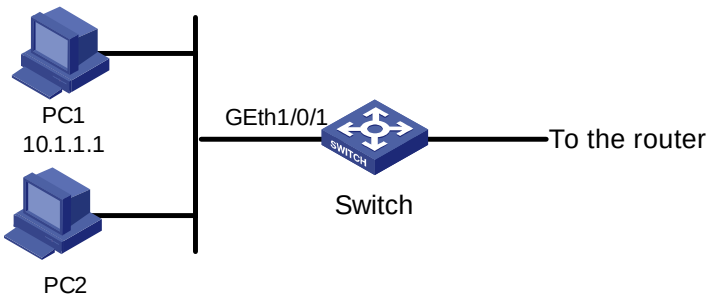
Examples for Applying ACLs to Hardware

Basic ACL Configuration Example

Network requirements

As shown in Figure 1-3, PC1 and PC2 connect to Switch through GigabitEthernet 1/0/1. PC1's IP address is 10.1.1.1. Apply an ACL on GigabitEthernet 1/0/1 to deny packets with the source IP address of 10.1.1.1 from 8:00 to 18:00 everyday.

Figure 1-3 Network diagram for basic ACL configuration



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<device> system-view
[device] time-range test 8:00 to 18:00 daily
```

Define ACL 2000 to filter packets with the source IP address of 10.1.1.1.

```
[device] acl number 2000
[device-acl-basic-2000] rule 1 deny source 10.1.1.1 0 time-range test
[device-acl-basic-2000] quit
```

Apply ACL 2000 on GigabitEthernet 1/0/1.

```
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] packet-filter inbound ip-group 2000
```

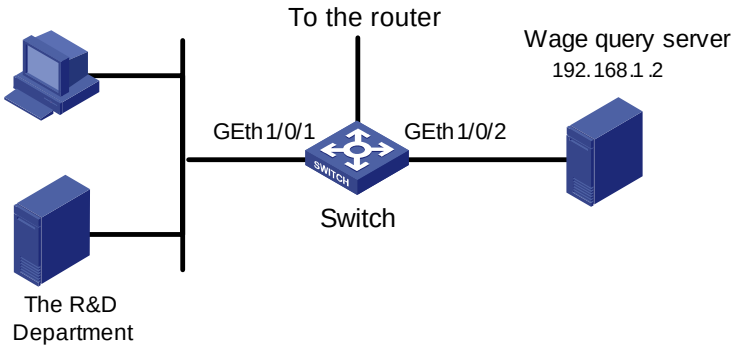
Advanced ACL Configuration Example

Network requirements

As shown in Figure 1-4, different departments of an enterprise are interconnected through Switch. The IP address of the wage query server is 192.168.1.2. The R&D department is connected to

GigabitEthernet 1/0/1 of Switch. Apply an ACL to deny requests from the R&D department and destined for the wage server during the working hours (8:00 to 18:00).

Figure 1-4 Network diagram for advanced ACL configuration



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<device> system-view
[device] time-range test 8:00 to 18:00 working-day
```

Define ACL 3000 to filter packets destined for wage query server.

```
[device] acl number 3000
[device-acl-adv-3000] rule 1 deny ip destination 192.168.1.2 0 time-range test
[device-acl-adv-3000] quit
```

Apply ACL 3000 on GigabitEthernet 1/0/1.

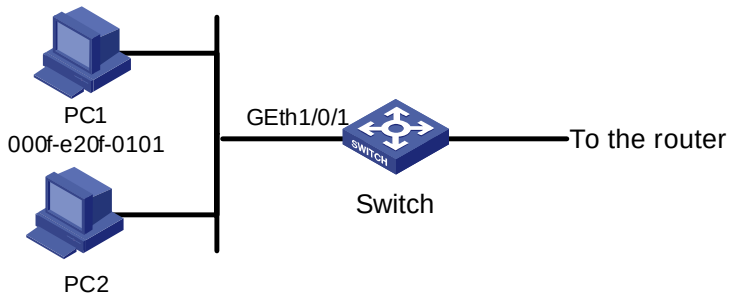
```
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] packet-filter inbound ip-group 3000
```

Layer 2 ACL Configuration Example

Network requirements

As shown in Figure 1-5, PC1 and PC2 connect to Switch through GigabitEthernet 1/0/1. PC1's MAC address is 000f-e20f-0101. Apply an ACL to filter packets with the source MAC address of 000f-e20f-0101 and the destination MAC address of 000f-e20f-0303 from 8:00 to 18:00 everyday.

Figure 1-5 Network diagram for Layer 2 ACL



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<device> system-view
[device] time-range test 8:00 to 18:00 daily
```

Define ACL 4000 to filter packets with the source MAC address of 000f-e20f-0101 and the destination MAC address of 000f-e20f-0303.

```
[device] acl number 4000
[device-acl-ethernetframe-4000] rule 1 deny source 000f-e20f-0101 ffff-ffff-ffff dest 000f-e20f-0303 ffff-ffff-ffff time-range test
[device-acl-ethernetframe-4000] quit
```

Apply ACL 4000 on GigabitEthernet 1/0/1.

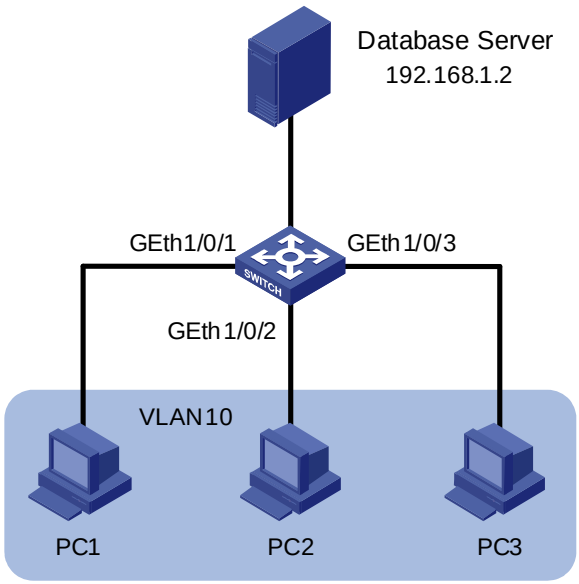
```
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] packet-filter inbound link-group 4000
```

Example for Applying an ACL to a VLAN

Network requirements

As shown in Figure 1-6, PC1, PC2 and PC3 belong to VLAN 10 and connect to the device through GigabitEthernet 1/0/1, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 respectively. The IP address of the database server is 192.168.1.2. Apply an ACL to deny packets from PCs in VLAN 10 to the database server from 8:00 to 18:00 in working days.

Figure 1-6 Network diagram for applying an ACL to a VLAN



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 in working days.

```
<device> system-view
[device] time-range test 8:00 to 18:00 working-day
```

Define an ACL to deny packets destined for the database server.

```
[device] acl number 3000
[device-acl-adv-3000] rule 1 deny ip destination 192.168.1.2 0 time-range test
[device-acl-adv-3000] quit
```

Apply ACL 3000 to VLAN 10.

```
[device] packet-filter vlan 10 inbound ip-group 3000
```

Table of Contents

1 QoS Configuration 1-1
Overview 1-1
Introduction to QoS 1-1
Traditional Packet Forwarding Service 1-1
New Applications and New Requirements 1-1
Major Traffic Control Techniques 1-2
QoS Supported by Devices 1-2
Traffic Classification 1-2
Precedence 1-3
Priority Trust Mode 1-5
Protocol Priority 1-8
Priority Marking 1-8
Traffic Policing and Traffic Shaping 1-8
Traffic Redirecting 1-10
VLAN Mapping 1-10
Queue Scheduling 1-10
Flow-based Traffic Accounting 1-13
Burst 1-13
Traffic mirroring 1-13
QoS Configuration 1-13
QoS Configuration Task List 1-13
Configuring Priority Trust Mode 1-14
Configuring Priority Mapping 1-15
Setting the Priority of Protocol Packets 1-18
Marking Packet Priority 1-19
Configuring Traffic Policing 1-20
Configuring Traffic Shaping 1-22
Configuring Traffic Redirecting 1-23
Configuring VLAN Mapping 1-25
Configuring Queue Scheduling 1-25
Collecting/Clearing Traffic Statistics 1-27
Enabling the Burst Function 1-29
Configuring Traffic Mirroring 1-29
Displaying and Maintaining QoS 1-32
QoS Configuration Example 1-33
Configuration Example of Traffic Policing 1-33

2 QoS Profile Configuration 2-1
Overview 2-1
Introduction to QoS Profile 2-1
QoS Profile Application Mode 2-1
QoS Profile Configuration 2-2
QoS Profile Configuration Task List 2-2
Configuring a QoS Profile 2-2

Applying a QoS Profile ····· 2-2
Displaying and Maintaining QoS Profile ····· 2-3
Configuration Example ····· 2-4
QoS Profile Configuration Example ····· 2-4

1 QoS Configuration



Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Overview

Introduction to QoS

Quality of service (QoS) is a concept generally existing in occasions with service supply and demand. It evaluates the ability to meet the need of the customers in service. Generally, the evaluation is not to grade precisely. Its purpose is to analyze the conditions where the service is the best and the conditions where the service still needs improvement and then to make improvements in the specified aspects.

In an internet, QoS evaluates the ability of the network to deliver packets. The evaluation on QoS can be based on different aspects because the network provides various services. Generally speaking, QoS is the evaluation on the service ability to support the core requirements such as delay, jitter, and packet loss ratio in the packet delivery.

Traditional Packet Forwarding Service

In traditional IP networks, packets are treated equally. That is, the FIFO (first in first out) policy is adopted for packet processing. Network resources required for packet forwarding is determined by the order in which packets arrive. All the packets share the resources of the network. Network resources available to the packets completely depend on the time they arrive. This service policy is known as Best-effort, which delivers the packets to their destination with the best effort, with no assurance and guarantee for delivery delay, jitter, packet loss ratio, reliability, and so on.

The traditional Best-Effort service policy is only suitable for applications insensitive to bandwidth and delay, such as WWW, file transfer and E-mail.

New Applications and New Requirements

With the expansion of computer network, more and more networks become part of the Internet. The Internet gains rapid development in terms of scale, coverage and user quantities. More and more users use the Internet as a platform for their services and for data transmission.

Besides the traditional applications such as WWW, E-mail, and FTP, new services are developed on the Internet, such as tele-education, telemedicine, video telephone, videoconference and

Video-on-Demand (VoD). Enterprise users expect to connect their regional branches together using VPN techniques for coping with daily business, for instance, accessing databases or manage remote equipments through Telnet.

All these new applications have one thing in common, that is, they have special requirements for bandwidth, delay, and jitter. For instance, bandwidth, delay, and jitter are critical for videoconference and VoD. As for other applications, such as transaction processing and Telnet, although bandwidth is not as critical, a too long delay may cause unexpected results. That is, they need to get serviced in time even if congestion occurs.

Newly emerging applications demand higher service performance from IP networks. In addition to simply delivering packets to their destinations, better network services are demanded, such as allocating dedicated bandwidth, reducing packet loss ratio, avoiding congestion, regulating network traffic, and setting priority of the packets. To meet those requirements, the network should be provided with better service capability.

Major Traffic Control Techniques

Traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance are the foundations for a network to provide differentiated services. Mainly they implement the following functions.

- Traffic classification identifies specific packets based on certain matching rules. It is a prerequisite for differentiated service.
- Traffic policing confines traffics to a specific specification. You can configure restriction or punishment measures against the traffics exceeding the specification to protect the benefits of carriers and to prevent network resources from being abused.
- Traffic shaping actively adjusts the output rate of traffics. It can enable the traffics to match the capacity of the downstream network devices, so as to prevent packets from being dropped and network congestion.
- Congestion management handles resource competition during network congestion. Generally, it adds packets to queues first, and then forwards the packets by using a scheduling algorithm.
- Congestion avoidance monitors the use of network resources and drops packets actively when congestion reaches certain degree. It relieves network load by adjusting traffics.

Traffic classification is the basis of all the above-mentioned traffic management technologies. It identifies packets using certain rules and makes differentiated services possible. Traffic policing, traffic shaping, congestion management, and congestion avoidance are methods for implementing network traffic control and network resource management. They are occurrences of differentiated services.

QoS Supported by Devices

Traffic Classification

Traffic here refers to service traffic; that is, all the packets passing the device.

Traffic classification means identifying packets that conform to certain characteristics according to certain rules. It is the foundation for providing differentiated services.

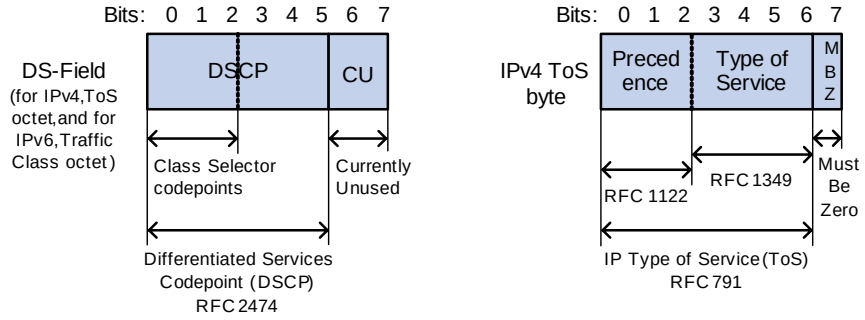
In traffic classification, the priority bit in the type of service (ToS) field in IP packet header can be used to identify packets of different priorities. The network administrator can also define traffic classification policies to identify packets by the combination of source address, destination address, MAC address, IP protocol or the port number of an application. Normally, traffic classification is done by checking the

information carried in packet header. Packet payload is rarely adopted for traffic classification. The identifying rule is unlimited in range. It can be a quintuplet consisting of source address, source port number, protocol number, destination address, and destination port number. It can also be simply a network segment.

Precedence

IP precedence, ToS precedence, and DSCP precedence

Figure 1-1 DS field and ToS byte



The ToS field in an IP header contains eight bits numbered 0 through 7, among which,

- The first three bits indicate IP precedence in the range 0 to 7.
- Bit 3 to bit 6 indicate ToS precedence in the range of 0 to 15.
- In RFC2474, the ToS field in IP packet header is also known as DS field. The first six bits (bit 0 through bit 5) of the DS field indicate differentiated service codepoint (DSCP) in the range of 0 to 63, and the last two bits (bit 6 and bit 7) are reserved.

Table 1-1 Description on IP precedence

IP Precedence (decimal)	IP Precedence (binary)	Description
0	000	Routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

In a network providing differentiated services, traffics are grouped into the following four classes, and packets are processed according to their DSCP values.

- Expedited Forwarding (EF) class: In this class, packets can be forwarded regardless of link share of other traffic. The class is suitable for preferential services with low delay, low packet loss ratio, low jitter, and assured bandwidth (such as virtual leased line);
- Assured forwarding (AF) class: This class is further divided into four subclasses (AF1/2/3/4) and a subclass is further divided into three drop priorities, so the AF service level can be segmented. The QoS rank of the AF class is lower than that of the EF class;

- Class selector (CS) class: This class comes from the IP ToS field and includes eight subclasses;
- Best Effort (BE) class: This class is a special class without any assurance in the CS class. The AF class can be degraded to the BE class if it exceeds the limit. Current IP network traffic belongs to this class by default.

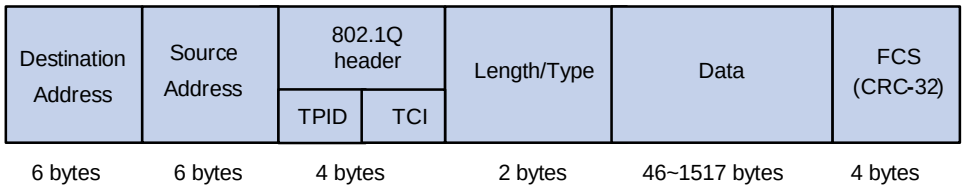
Table 1-2 Description on DSCP precedence values

DSCP value (decimal)	DSCP value (binary)	Description
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

802.1p priority

802.1p priority lies in Layer 2 packet headers and is applicable to occasions where the Layer 3 packet header does not need analysis but QoS must be assured at Layer 2.

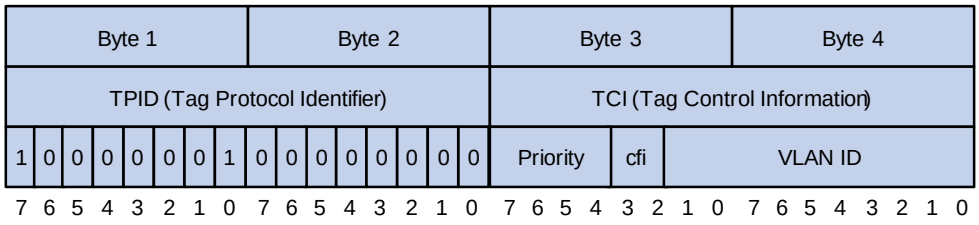
Figure 1-2 An Ethernet frame with an 802.1Q tag header



As shown in the figure above, each host supporting 802.1Q protocol adds a 4-byte 802.1Q tag header after the source address of the former Ethernet frame header when sending packets.

The 4-byte 802.1Q tag header consists of the tag protocol identifier (TPID, two bytes in length), whose value is 0x8100, and the tag control information (TCI, two bytes in length). Figure 1-3 describes the detailed contents of an 802.1Q tag header.

Figure 1-3 802.1Q tag headers



In the figure above, the priority field (three bits in length) in TCI is 802.1p priority (also known as CoS precedence), which ranges from 0 to 7.

Table 1-3 Description on 802.1p priority

802.1p priority (decimal)	802.1p priority (binary)	Description
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

The precedence is called 802.1p priority because the related applications of this precedence are defined in detail in the 802.1p specifications.

Priority Trust Mode

A device can assign different types of precedence to the packets it receives as configured, such as 802.1p precedence, DSCP precedence, local precedence, and drop precedence.

Among the above-mentioned precedence types:

- The local precedence is only of local significance. A local precedence corresponds to a specific output queue. Packets with higher local precedence values take precedence over those with lower precedence values and will be processed preferentially.
- The drop precedence determines which packets are dropped preferentially. The higher the drop precedence, the more likely a packet is dropped.

Note

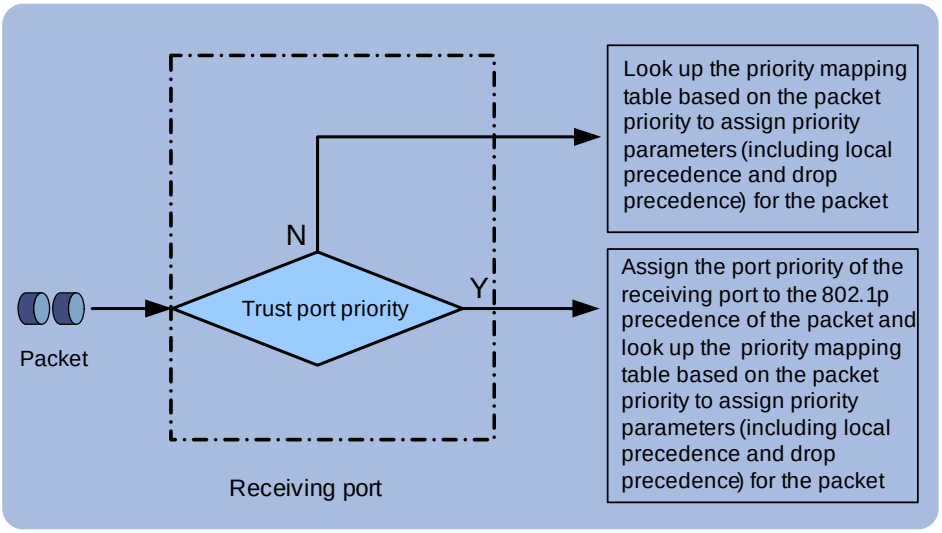
The device does not support marking drop precedence for packets.

A device can operate in one of the following two priority trust modes when assigning precedence to received packets:

- Packet priority trusted mode
- Port priority trusted mode

In terms of priority trust mode, the priority mapping process is shown in Figure 1-4.

Figure 1-4 Assigning precedence to received packets in different trust modes



As for packet priority trusted mode, you can configure to trust the following packet priority:

- 802.1p precedence
- DSCP precedence

Trusting the 802.1p precedence

In this mode, you can specify to process the received packets in one of the following two ways.

- Keeping the original packet precedence unchanged (the default mode)
- Replacing the original packet precedence with the corresponding one (the **automap** mode).

If a packet does not carry 802.1p precedence, the device uses the priority of the receiving port as the 802.1p precedence of the packet and then looks up the COS-precedence-to-other-precedence mapping table for the corresponding precedence.

Trusting the DSCP precedence

In this mode, you can specify to process the received packets in one of the following ways.

- Keeping the original packet precedence unchanged (the default mode)
- Replacing the original packet precedence with the corresponding one (the **automap** mode)
- Looking up the DSCP-precedence-to-DSCP-precedence mapping table for the local DSCP precedence and then looking up the DSCP-precedence-to-other-precedence mapping table based on the new DSCP precedence for the one to be assigned to the packets (the **remap** mode)

The devices provide COS-precedence-to-other-precedence, DSCP-precedence-to-other-precedence, and DSCP-precedence-to-DSCP- precedence mapping tables for priority mapping. Table 1-4 through Table 1-6 list the default settings of these tables.

Table 1-4 The default COS-precedence-to-other-precedence mapping table of the devices

802.1p precedence	Target local precedence	Target drop precedence	Target DSCP precedence
0	2	0	16
1	0	0	0
2	1	0	8
3	3	0	24
4	4	0	32
5	5	0	40
6	6	0	48
7	7	0	56

Table 1-5 The default DSCP-precedence-to-other-precedence mapping table of the devices

DSCP precedence	Target local precedence	Target drop precedence	Target 802.1p precedence
0 to 7	0	1	1
8 to 15	1	1	2
16 to 23	2	1	0
24 to 31	3	1	3
32 to 39	4	0	4
40 to 47	5	0	5
48 to 55	6	0	6
56 to 63	7	0	7

Table 1-6 The default DSCP-precedence-to-DSCP-precedence mapping table of the devices

DSCP precedence	Target DSCP precedence
0	0
1	1
2	2
3	3
...	...
61	61
62	62
63	63

Protocol Priority

Protocol packets carry their own priority. You can modify the priority of a protocol packet to implement QoS.

Priority Marking

The priority marking function is to use ACL rules in traffic classification and reassign the priority for the packets matching the ACL rules.

Traffic Policing and Traffic Shaping

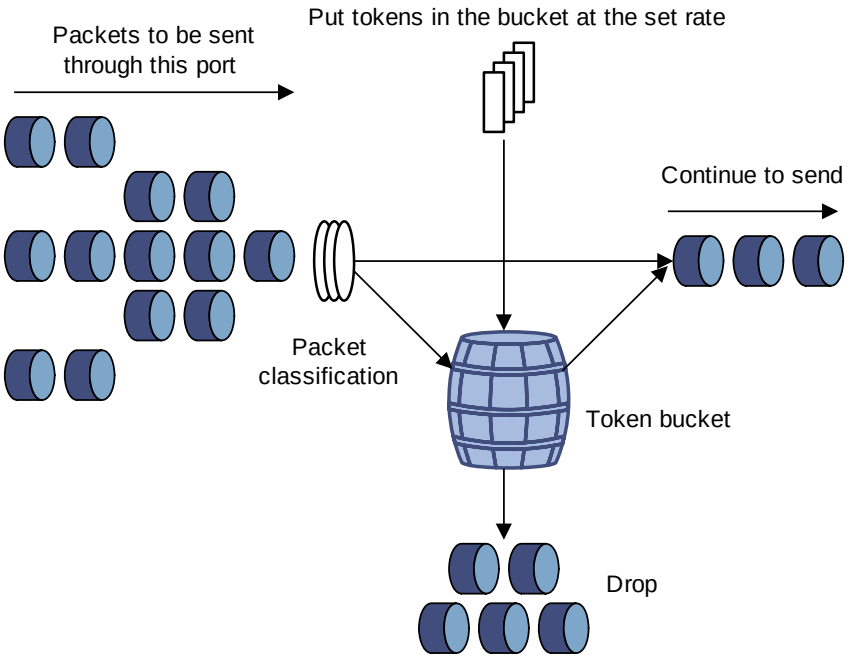
The network will be made more congested by plenty of continuous burst packets if the traffic of each user is not limited. The traffic of each user must be limited in order to make better use of the limited network resources and provide better service for more users. For example, a traffic flow can be limited to get only its committed resources during a time period to avoid network congestion caused by excessive bursts.

Traffic policing and traffic shaping is each a kind of traffic control policy used to limit the traffic and the resource occupied by supervising the traffic. The regulation policy is implemented according to the evaluation result on the premise of knowing whether the traffic exceeds the specification when traffic policing or traffic shaping is performed. Normally, token bucket is used for traffic evaluation.

Token bucket

The token bucket can be considered as a container with a certain capacity to hold tokens. The system puts tokens into the bucket at the set rate. When the token bucket is full, the extra tokens will overflow and the number of tokens in the bucket stops increasing.

Figure 1-5 Evaluate the traffic with the token bucket



Evaluating the traffic with the token bucket

When token bucket is used for traffic evaluation, the number of the tokens in the token bucket determines the amount of the packets that can be forwarded. If the number of tokens in the bucket is enough to forward the packets, the traffic is conforming to the specification; otherwise, the traffic is nonconforming or excess.

Parameters concerning token bucket include:

- Average rate: The rate at which tokens are put into the bucket, namely, the permitted average rate of the traffic. It is generally set to committed information rate (CIR).
- Burst size: The capacity of the token bucket, namely, the maximum traffic size that is permitted in each burst. It is generally set to committed burst size (CBS). The set burst size must be greater than the maximum packet length.

One evaluation is performed on each arriving packet. In each evaluation, if the number of tokens in the bucket is enough, the traffic is conforming to the specification and you must take away some tokens whose number is corresponding to the packet forwarding authority; if the number of tokens in the bucket is not enough, it means that too many tokens have been used and the traffic is excess.

Traffic policing

The typical application of traffic policing is to supervise specific traffic into the network and limit it to a reasonable range, or to "discipline" the extra traffic. In this way, the network resources and the interests of the operators are protected. For example, you can limit HTTP packets to be within 50% of the network bandwidth. If the traffic of a certain connection is excess, traffic policing can choose to drop the packets or to reset the priority of the packets.

Traffic policing is widely used in policing the traffic into the network of internet service providers (ISPs). Traffic policing can identify the policed traffic and perform pre-defined policing actions based on different evaluation results. These actions include:

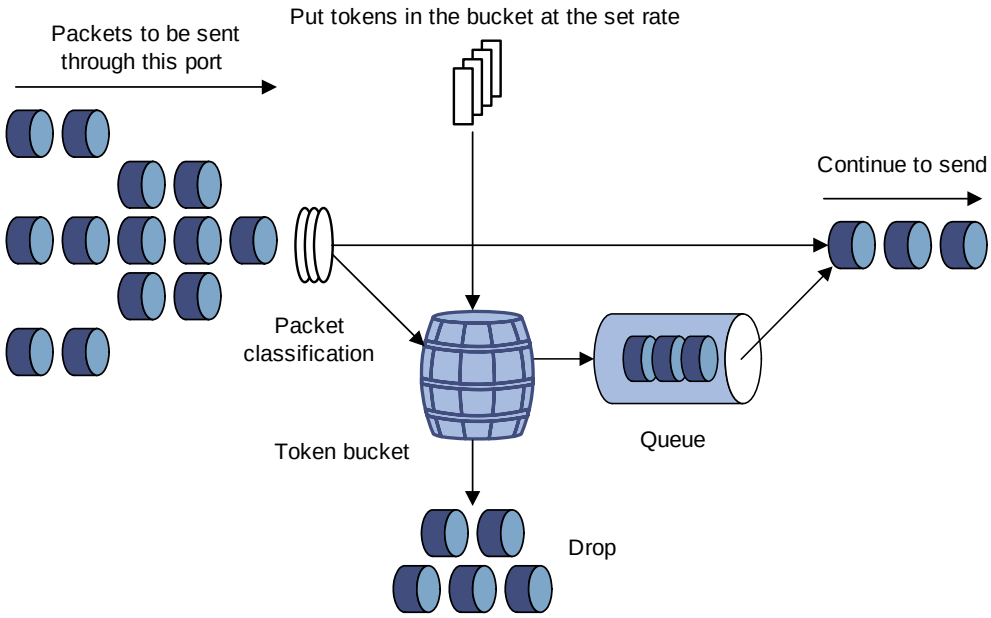
- Discarding the nonconforming packets.
- Forwarding the conforming packets or nonconforming packets.
- Marking the conforming packets or nonconforming packets with 802.1p precedence and then forwarding the packets.
- Marking the conforming packets or nonconforming packets with DSCP precedence and forwarding the packets.

Traffic shaping

Traffic shaping is a measure to regulate the output rate of traffic actively. Its typical application is to control local traffic output based on the traffic policing indexes of downstream network nodes.

The major difference between traffic shaping and traffic policing is that the packets to be dropped in traffic policing are cached in traffic shaping——usually in buffers or queues, as shown in Figure 1-6. When there are enough tokens in the token bucket, the cached packets are sent out evenly. Another difference between traffic policing and traffic shaping is that traffic shaping may increase the delay while traffic policing hardly increases the delay.

Figure 1-6 Diagram for traffic shaping



For example, if the device A sends packets to the device B. The device B will perform traffic policing on packets from the device A to drop the packets beyond the specification.

In order to avoid meaningless packet loss, you can perform traffic shaping on the packets on the egress of the device A and cache the packets beyond the traffic policing specification in the device A. When the next packets can be sent, the packets cached in the buffer queues will be taken out and sent. In this way, all the packets sent to the device B conforms to the traffic specification of the device B.

Traffic Redirecting

Traffic redirecting identifies traffic using ACLs and redirects the matched packets to specific ports. By traffic redirecting, you can change the way in which a packet is forwarded to achieve specific purposes.

VLAN Mapping

VLAN mapping identifies traffics using ACLs and maps the VLAN tags carrier in matched packets to specific VLAN tags. By employing VLAN mapping on a device connecting user networks to the carrier network, you can map the VLAN tags of specific user network packets to those of specific VLANs in the carrier network, thus meeting the requirements of the carrier network.

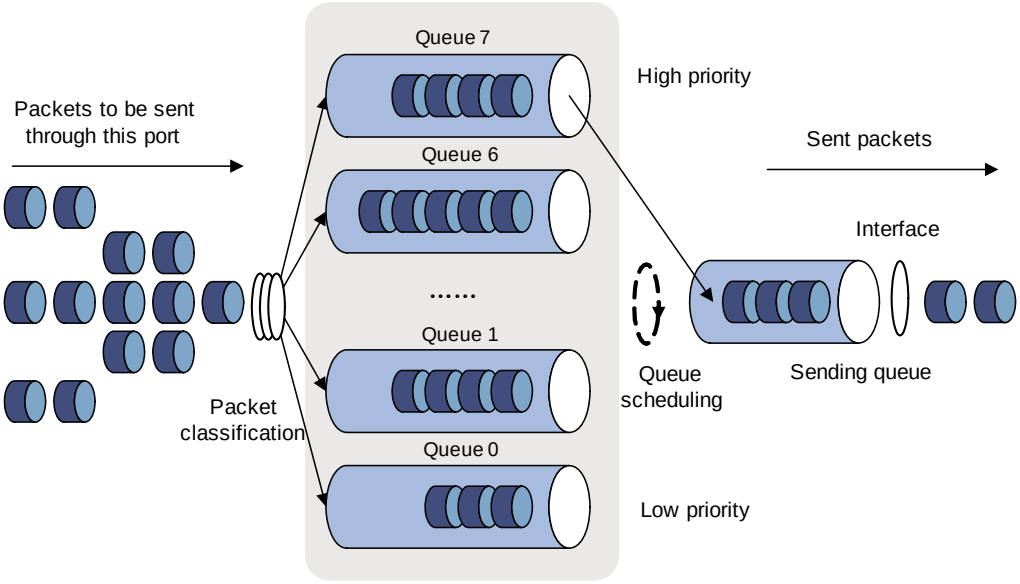
Queue Scheduling

When the network is congested, the problem that many packets compete for resources must be solved, usually through queue scheduling.

In the following section, strict priority (SP) queues, weighted round robin (WRR),and SDWRR (Shaped Deficit WRR) queues are introduced.

1) SP queuing

Figure 1-7 Diagram for SP queuing



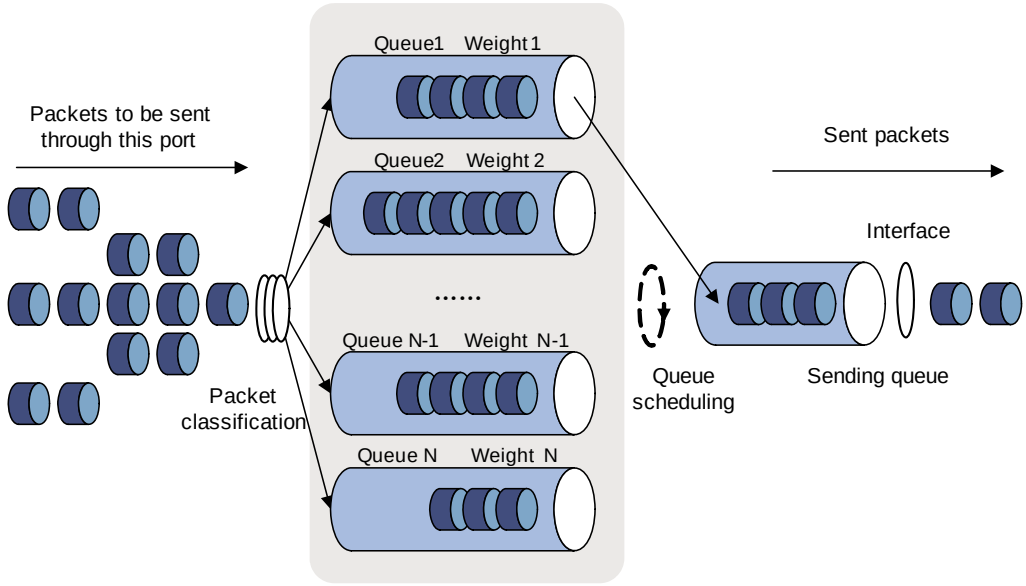
SP queue-scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay. Assume that there are eight output queues on the port and the preferential queue classifies the eight output queues on the port into eight classes, which are queue7, queue6, queue5, queue4, queue3, queue2, queue1, and queue0. Their priorities decrease in order.

In queue scheduling, SP sends packets in the queue with higher priority strictly following the priority order from high to low. When the queue with higher priority is empty, packets in the queue with lower priority are sent. You can put critical service packets into the queues with higher priority and put non-critical service (such as e-mail) packets into the queues with lower priority. In this case, critical service packets are sent preferentially and non-critical service packets are sent when critical service groups are not sent.

The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be “starved” because they are not served.

2) WRR queuing

Figure 1-8 Diagram for WRR queuing



WRR queue-scheduling algorithm schedules all the queues in turn and every queue can be assured of a certain service time. Assume there are eight priority queues on a port. WRR configures a weight value for each queue, which is w7, w6, w5, w4, w3, w2, w1, and w0. The weight value indicates the proportion of obtaining resources. On a 100 M port, configure the weight value of WRR queue-scheduling algorithm to 50, 50, 30, 30, 10, 10, 10, and 10 (corresponding to w7, w6, w5, w4, w3, w2, w1, and w0 in order). In this way, the queue with the lowest priority can get 5 Mbps bandwidth at least, and the disadvantage of SP queue-scheduling that the packets in queues with lower priority may not get service for a long time is avoided. Another advantage of WRR queue is that: though the queues are scheduled in order, the service time for each queue is not fixed; that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use.

3) SDWRR

Comparing with WRR queue, SDWRR queue further optimizes the delay and variation for different queues.

For example, configure the weight value of queue0 and queue1 to 5 and 3 respectively. The processing procedures of WRR and SDWRR are as follows:

- WRR: The packets whose weight value is 3 in queue1 are scheduled only after the packets whose weight value is 5 in the queue0 are scheduled. If there is a wide difference between the weight values of two queues, the queue with high weight value will cause great delay and variation for the queue with low weight value.
- SDWRR: Two queues are scheduled in turn. Packets whose weight value is 1 in queue0 are scheduled first, and then packets whose weight value is 1 in queue1 are scheduled. The procedure is repeated until the scheduling for one queue is over, and then SDWRR will schedule packets with the left weight values in the other queue. The detailed scheduling sequence is described in the Table 1-7.

Table 1-7 Queue-scheduling sequence of SDWRR

Scheduling algorithm	Queue-scheduling sequence	Description
WRR	0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1	0 indicates packets in queue0 1 indicates packets in queue1
SDWRR	0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0	

Flow-based Traffic Accounting

The function of flow-based traffic accounting is to use ACL rules in traffic classification and perform traffic accounting on the packets matching the ACL rules. You can get the statistics of the packets you are interested in through this function.

Burst

The Burst function can provide better packet cache function and traffic forwarding performance. It is suitable for networks where

- Large amount of broadcast/multicast packets and large burst traffic exist.
- Packets of high-rate links are forwarded to low-rate links or packets of multiple links with the equal rates are forwarded to a single link that is of the same rate as that of the incoming links.

Although the burst function helps reduce the packet loss ratio and improve packet processing capability in the networks mentioned above, it may affect QoS performance. So, use this function with caution.

Traffic mirroring

Traffic mirroring identifies traffic using ACLs and duplicates the matched packets to the destination port. For information about port mirroring, refer to the Mirroring module of this manual.

QoS Configuration

QoS Configuration Task List

Complete the following tasks to configure QoS:

Task	Remarks
Configuring Priority Trust Mode	Optional
Configuring Priority Mapping	Optional
Setting the Priority of Protocol Packets	Optional
Marking Packet Priority	Optional
Configuring Traffic Policing	Optional
Configuring Traffic Shaping	Optional
Configuring Traffic Redirecting	Optional
Configuring VLAN Mapping	Optional
Configuring Queue Scheduling	Optional
Collecting/Clearing Traffic Statistics	Optional

Task	Remarks
Enabling the Burst Function	Optional
Configuring Traffic Mirroring	Optional

Configuring Priority Trust Mode

Refer to Priority Trust Mode for introduction to priority trust mode.

Configuration prerequisites

- The priority trust mode to be adopted is determined.
- The port where priority trust mode is to be configured is determined.
- The port priority value is determined.

Configuration procedure

Follow these steps to configure to trust port priority:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the port priority	**priority** *priority-level*	Optional 0 by default

Follow these steps to configure to trust 802.1p precedence:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure to trust 802.1p precedence	**priority-trust cos** [**automap**]	Required By default, port priority is trusted.

Follow these steps to configure to trust DSCP precedence:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure to trust DSCP precedence	**priority-trust dscp** [**automap** | **remap**]	Required By default, port priority is trusted.

Configuration example

- Configure to trust port priority on GigabitEthernet 1/0/1 and set the priority of GigabitEthernet 1/0/1 to 7.

Configuration procedure:

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] priority 7
```

- Configure to trust 802.1p precedence on GigabitEthernet 1/0/1.

Configuration procedure:

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] priority-trust cos
```

- Configure to trust DSCP precedence on GigabitEthernet 1/0/1.

Configuration procedure:

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] priority-trust dscp
```

Configuring Priority Mapping

You can modify the COS-precedence-to-other-precedence, DSCP-precedence-to-other-precedence, and DSCP-precedence-to-DSCP-precedence mapping tables as required to mark packets with different priorities.

Configuration prerequisites

The target COS-precedence-to-other-precedence, DSCP-precedence-to-other-precedence, and DSCP-precedence-to-DSCP-precedence mapping tables are determined.

Configuration procedure

Follow these steps to configure the COS-precedence-to-other-precedence mapping table:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure COS-precedence-to-local-precedence mapping table	**qos cos-local-precedence-map** *cos0-map-local-prec cos1-map-local-prec cos2-map-local-prec cos3-map-local-prec cos4-map-local-prec cos5-map-local-prec cos6-map-local-prec cos7-map-local-prec*	Required
Configure COS-precedence-to-drop-precedence mapping table	**qos cos-drop-precedence-map** *cos0-map-drop-prec cos1-map-drop-prec cos2-map-drop-prec cos3-map-drop-prec cos4-map-drop-prec cos5-map-drop-prec cos6-map-drop-prec cos7-map-drop-prec*	Required

To do…	Use the command…	Remarks
Configure COS-precedence-to-DSCP -precedence mapping table	**qos cos-dscp-map** *cos0-map-dscp cos1-map-dscp cos2-map-dscp cos3-map-dscp cos4-map-dscp cos5-map-dscp cos6-map-dscp cos7-map-dscp*	Required

Follow these steps to configure the DSCP-precedence-to-other-precedence mapping table:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure DSCP-precedence-to-local -precedence mapping table	**qos dscp-local-precedence-map** *dscp-list* **:** *local-precedence*	Required
Configure DSCP-precedence-to-drop -precedence mapping table	**qos dscp-drop-precedence-map** *dscp-list* **:** *drop-precedence*	Required
Configure DSCP-precedence-to-COS -precedence mapping table	**qos dscp-cos-map** *dscp-list* **:** *cos-value*	Required

Follow these steps to configure the DSCP-precedence-to-DSCP-precedence mapping table:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure DSCP-precedence-to-DSCP -precedence mapping table	**qos dscp-dscp-map** *dscp-list* **:** *dscp-value*	Required

Configuration example

- Configure the COS-precedence-to-local-precedence mapping relationship for a device as follows: 0 to 2, 1 to 3, 2 to 4, 3 to 1, 4 to 7, 5 to 0, 6 to 5, and 7 to 6.
- Display the configuration.

Configuration procedure:

```
<device> system-view
[device] qos cos-local-precedence-map 2 3 4 1 7 0 5 6
[device] display qos cos-local-precedence-map
 cos-local-precedence-map:
            cos(802.1p) :      0     1     2     3     4     5     6     7
------------------------------------------------------------------------------
local precedence(queue) :      2     3     4     1     7     0     5     6
```

- Configure the DSCP-precedence-to-local-precedence mapping relationship for a device as follows: 0 through 7 to 2, 8 through 15 to 3, 16 through 23 to 4, 24 through 31 to 1, 32 through 39 to 7, 40 through 47 to 0, 48 through 55 to 5, and 56 through 63 to 6.
- Display the configuration.

```
<device> system-view
[device] qos dscp-local-precedence-map 0 1 2 3 4 5 6 7 : 2
```

```
[device] qos dscp-local-precedence-map 8 9 10 11 12 13 14 15 : 3
[device] qos dscp-local-precedence-map 16 17 18 19 20 21 22 23 : 4
[device] qos dscp-local-precedence-map 24 25 26 27 28 29 30 31 : 1
[device] qos dscp-local-precedence-map 32 33 34 35 36 37 38 39 : 7
[device] qos dscp-local-precedence-map 40 41 42 43 44 45 46 47 : 0
[device] qos dscp-local-precedence-map 48 49 50 51 52 53 54 55 : 5
[device] qos dscp-local-precedence-map 56 57 58 59 60 61 62 63 : 6
<device> display qos dscp-local-precedence-map
 dscp-local-precedence-map:
             dscp : local-precedence(queue)
 ---------------------------------------------
                0 :            2
                1 :            2
                2 :            2
                3 :            2
                4 :            2
                5 :            2
                6 :            2
                7 :            2
                8 :            3
                9 :            3
               10 :            3
               11 :            3
               12 :            3
               13 :            3
               14 :            3
               15 :            3
               16 :            4
               17 :            4
               18 :            4
               19 :            4
               20 :            4
               21 :            4
               22 :            4
               23 :            4
               24 :            1
               25 :            1
               26 :            1
               27 :            1
               28 :            1
               29 :            1
               30 :            1
               31 :            1
               32 :            7
               33 :            7
               34 :            7
               35 :            7
               36 :            7
```

```
37 :            7
38 :            7
39 :            7
40 :            0
41 :            0
42 :            0
43 :            0
44 :            0
45 :            0
46 :            0
47 :            0
48 :            5
49 :            5
50 :            5
51 :            5
52 :            5
53 :            5
54 :            5
55 :            5
56 :            6
57 :            6
58 :            6
59 :            6
60 :            6
61 :            6
62 :            6
63 :            6
```

Setting the Priority of Protocol Packets

Refer to Protocol Priority for information about priority of protocol packets.

Configuration prerequisites

- The protocol type is determined.
- The priority value is determined.

Configuration procedure

Follow these steps to set the priority for specific protocol packets:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the priority for specific protocol packets	**protocol-priority protocol-type** *protocol-type* { **ip-precedence** *ip-precedence* | **dscp** *dscp-value* }	Required You can modify the IP precedence or DSCP precedence of the corresponding protocol packets. On a device, you can set the priority for protocol packets of Telnet, SNMP, and ICMP.

Configuration example

- Set the IP precedence of ICMP packets to 3.
- Display the configuration.

Configuration procedure:

```
<device> system-view
[device] protocol-priority protocol-type icmp ip-precedence 3
[device] display protocol-priority
Protocol: icmp
  IP-Precedence: flash(3)
```

Marking Packet Priority

Refer to Priority Marking for information about marking packet priority.

Marking packet priority can be implemented in the following two ways:

- Through traffic policing

When configuring traffic policing, you can define the action of marking the 802.1p priority and DSCP precedence for packets exceeding the traffic specification. Refer to Configuring Traffic Policing.

- Through the **traffic-priority** command

You can use the **traffic priority** command to mark the 802.1p priority and DSCP precedence of the packets.

Configuration prerequisites

The following items are defined or determined before the configuration:

- The ACL rules used for traffic classification are specified. Refer to the ACL module of this manual for related information.
- The type and value of the precedence to be marked for the packets matching the ACL rules are determined.

Configuration procedure

You can mark priority for all the packets matching specific ACL rules, or for packets that match specific ACL rules and are of a VLAN, of a port group, or pass a port.

Follow these steps to mark the priority for the packets matching specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Mark the priorities for packets matching specific ACL rules	**traffic-priority inbound** *acl-rule* { **dscp** *dscp-value* | **cos** *cos-value* }	Required

Follow these steps to mark the priority for packets that are of a VLAN and match specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Mark the priorities for packets matching specific ACL rules	**traffic-priority vlan** *vlan-id* **inbound** *acl-rule* { **dscp** *dscp-value* | **cos** *cos-value* }	Required

Follow these steps to mark the priority for packets that are of a port group and match specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter port group view	**port-group** *group-id*	—
Mark the priorities for packets matching specific ACL rules	**traffic-priority inbound** *acl-rule* { **dscp** *dscp-value* | **cos** *cos-value* }	Required

Follow these steps to mark the priority for packets passing a port and matching specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Mark the priorities for packets matching specific ACL rules	**traffic-priority inbound** *acl-rule* { **dscp** *dscp-value* | **cos** *cos-value* }	Required

Caution

As the priority of traffic classification rules is higher than that of the default rules used for processing protocol packets, marking priority for all the packets or packets of a VLAN may affect device management that is implemented through Telnet and so on.

Configuration example

- GigabitEthernet 1/0/1 belongs to VLAN 2 and is connected to the 10.1.1.0/24 network segment.
- Mark the DSCP precedence as 56 for the packets from the 10.1.1.0/24 network segment.

1) Method I

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[device-acl-basic-2000] quit
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] traffic-priority inbound ip-group 2000 dscp 56
```

2) Method II

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[device-acl-basic-2000] quit
[device] traffic-priority vlan 2 inbound ip-group 2000 dscp 56
```

Configuring Traffic Policing

Refer to Traffic Policing and Traffic Shaping for information about traffic policing.

Configuration prerequisites

- The ACL rules used for traffic classification are defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The rate limit for traffic policing, and the actions for the packets exceeding the rate limit are determined.

Configuration procedure

You can configure traffic policing for all the packets matching specific ACL rules, or for the packets that match specific ACL rules and are of a VLAN, of a port group, or pass a port.

Follow these steps to configure traffic policing for all the packets matching specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure traffic policing	**traffic-limit inbound** *acl-rule target-rate* [**conform** *con-action*] [**exceed** *exceed-action*] [**meter-statistic**]	Required By default, traffic policing is disabled.
Clear the traffic policing statistics	**reset traffic-limit inbound** *acl-rule*	Optional

Follow these steps to configure traffic policing for packets that are of a VLAN and match specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure traffic policing	**traffic-limit vlan** *vlan-id* **inbound** *acl-rule target-rate* [**conform** *con-action*] [**exceed** *exceed-action*] [**meter-statistic**]	Required By default, traffic policing is disabled.
Clear the traffic policing statistics	**reset traffic-limit vlan** *vlan-id* **inbound** *acl-rule*	Optional

Follow these steps to configure traffic policing for packets that are of a port group and match specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter port group view	**port-group** *group-id*	—
Configure traffic policing	**traffic-limit inbound** *acl-rule target-rate* [**conform** *con-action*] [**exceed** *exceed-action*] [**meter-statistic**]	Required By default, traffic policing is disabled.
Clear the traffic policing statistics	**reset traffic-limit inbound** *acl-rule*	Optional

Follow these steps to configure traffic policing for packets passing a port and matching specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure traffic policing	**traffic-limit inbound** *acl-rule target-rate* [**conform** *con-action*] [**exceed** *exceed-action*] [**meter-statistic**]	Required By default, traffic policing is disabled.
Clear the traffic policing statistics	**reset traffic-limit inbound** *acl-rule*	Optional

Caution

As the priority of traffic classification rules is higher than that of the default rules used for processing protocol packets, configuring traffic policing for all the packets or packets of a VLAN may affect device management that is implemented through Telnet and so on.

Configuration example

- GigabitEthernet 1/0/1 belongs to VLAN 2 and is connected to the 10.1.1.0/24 network segment
- Perform traffic policing on the packets from the 10.1.1.0/24 network segment, setting the rate to 128 kbps
- Mark the DSCP precedence as 56 for the inbound packets exceeding the rate limit.

1) Method I

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[device-acl-basic-2000] quit
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] traffic-limit inbound ip-group 2000 128 exceed remark-dscp 56
```

2) Method II

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[device-acl-basic-2000] quit
[device] traffic-limit vlan 2 inbound ip-group 2000 128 exceed remark-dscp 56
```

Configuring Traffic Shaping

Refer to Traffic Policing and Traffic Shaping for information about traffic shaping.

Configuration prerequisites

- The queue for which traffic shaping is to be performed is determined.
- The maximum traffic rate and the burst size are determined.
- The port where traffic shaping is to be configured is determined.

Configuration procedure

Follow these steps to configure traffic shaping:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure traffic shaping	**traffic-shape** [**queue** *queue-id*] *max-rate burst-size*	Required Traffic shaping is not enabled by default. Traffic shaping can be performed in one of the following two modes: • With the **queue** *queue-id* keyword and argument combination not specified, traffic shaping is performed for all the traffic. • With the **queue** *queue-id* keyword and argument combination specified, traffic shaping is performed for the traffic in the specific output queue.

Configuration examples

Perform traffic shaping for all the traffic to be transmitted through GigabitEthernet 1/0/1, with the maximum traffic rate being 640 kbps and the burst size being 16 kbytes.

```
<device> system-view
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] traffic-shape 640 16
```

Configuring Traffic Redirecting

Refer to Traffic Redirecting for information about traffic redirecting.

Configuration prerequisites

- The ACL rules used for traffic classification are defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The port which the packets matching the specified ACL rules are to be redirected to is determined.

Configuration procedure

You can redirect all the packets matching specific ACL rules, or packets that match specific ACL rules and are of a VLAN, of a port group, or pass a port.

Follow these steps to redirect all the packets matching specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure traffic redirecting	**traffic-redirect inbound** *acl-rule* **interface** *interface-type interface-number*	Required

Follow these steps to redirect packets that are of a VLAN and match specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure traffic redirecting	**traffic-redirect vlan** *vlan-id* **inbound** *acl-rule* **interface** *interface-type interface-number*	Required

Follow these steps to redirect packets that are of a port group and match specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter port group view	**port-group** *group-id*	—
Configure traffic redirecting	**traffic-redirect inbound** *acl-rule* **interface** *interface-type interface-number*	Required

Follow these steps to redirect packets passing a port and matching specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure traffic redirecting	**traffic-redirect inbound** *acl-rule* **interface** *interface-type interface-number*	Required

Note

If the traffic is redirected to a Combo port in down state, the system automatically redirects the traffic to the port corresponding to the Combo port in up state. Refer to the Port Basic Configuration module of this manual for information about Combo ports.

Caution

As the priority of traffic classification rules is higher than that of the default rules used for processing protocol packets, redirecting all the packets or packets of a VLAN may affect device management that is implemented through Telnet and so on.

Configuration example

- GigabitEthernet 1/0/1 belongs to VLAN 2 and is connected to the 10.1.1.0/24 network segment.
- Redirect all the packets from the 10.1.1.0/24 network segment to GigabitEthernet 1/0/7.

1) Method I

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
```

```
[device-acl-basic-2000] quit
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1]   traffic-redirect   inbound   ip-group   2000   interface
GigabitEthernet1/0/7
```

2) Method II

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[device-acl-basic-2000] quit
[device] traffic-redirect vlan 2 inbound ip-group 2000 interface GigabitEthernet1/0/7
```

Configuring VLAN Mapping

Refer to VLAN Mapping for information about VLAN mapping.

Configuration prerequisites

- The ACL rules used for traffic classification are defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The VLAN ID to be marked is determined.
- The ports on which the configuration is to be performed are determined.

Configuration procedure

Follow these steps to configure VLAN mapping:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure VLAN mapping	**traffic-remark-vlanid inbound** *acl-rule* **remark-vlan** *vlan-id* **untagged-packet**	Required By default, VLAN mapping is not configured.

Configuration example

- GigabitEthernet 1/0/1 belongs to VLAN 2 and is connected to the 10.1.1.0/24 network segment.
- Configure VLAN mapping for all the packets sourced from the 10.1.1.0/24 network segment to map the VLAN IDs of these packets to 1001.

Configuration procedure :

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[device-acl-basic-2000] quit
[device] interface GigabitEthernet 1/0/1
[device-GigabitEthernet1/0/1] traffic-remark-vlanid inbound ip-group 2000 remark-vlan 1001
```

Configuring Queue Scheduling

Refer to Queue Scheduling for information about queue scheduling.

Configuration prerequisites

The algorithm for queue scheduling to be used and the related parameters are determined.

Configuration procedure

Follow these steps to configure SP queue scheduling algorithm:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure SP queue scheduling algorithm	**undo queue-scheduler** [*queue-id*] &<1-8>	Optional By default, SP queue scheduling algorithm is adopted on all the output queues of a port.

Follow these steps to configure SDWRR queue scheduling algorithm:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure SDWRR queue scheduling algorithm	**queue-scheduler wrr** { **group1** { *queue-id queue-weight* } &<1-8> | **group2** { *queue-id queue-weight* } &<1-8> }*	Required By default, SP queue scheduling algorithm is adopted on all the output queues of a port.

A port on a device can accommodate up to eight output queues. You can configure to use SP queue scheduling algorithm, SDWRR queue scheduling algorithm, or combine the two as required.

- With SDWRR queue scheduling algorithm adopted, the output queues of a port can be assigned to group 1 and group 2. The two groups are scheduled using SP algorithm. For example, you can assign queue 0, queue 1, queue 2, and queue 3 to group 1, and assign queue 4, queue 5, queue 6, and queue 7 to group 2. The queues in group 2 are scheduled preferentially using WRR queue scheduling algorithm. Queues in group 1 are scheduled using WRR queue scheduling algorithm only when all the queues in group 2 are empty.
- With both SP and SDWRR queue scheduling algorithms adopted, groups are scheduled using SP algorithm. Assume that queue 0 and queue 1 are scheduled using SP algorithm; queue 2, queue 3, and queue 4 are assigned to group 1; queue 5, queue 6, and queue 7 are assigned to group 2. The queues in group 2 are scheduled preferentially using WRR queue scheduling algorithm. When all the queues in group 2 are empty, queues in group 1 are scheduled using WRR queue scheduling algorithm. Then, queue 1 is scheduled, and then queue 0.

 **Note**

When using SDWRR or SP+SDWRR combination for queue scheduling, you are recommended to assign queues with successive queue numbers to the same scheduling group.

Configuration example

Configure a device to adopt SP+SDWRR combination for queue scheduling, assigning queue 3, queue 4, and queue 5 to WRR scheduling group 1, with the weigh of 20, 20 and 30; assigning queue 0, queue 1, and queue 2 to WRR scheduling group 2, with the weight 20, 20, and 40; using SP for scheduling queue 6 and queue 7. Display the configuration information after configuration.

Configuration procedure:

```
<device> system-view
[device] queue-scheduler wrr group1 3 20 4 20 5 30 group2 0 20 1 20 2 40
[device] display queue-scheduler
QID:   scheduling-group     weight
-----------------------------------
  0 :   wrr , group2           20
  1 :   wrr , group2           20
  2 :   wrr , group2           40
  3 :   wrr , group1           20
  4 :   wrr , group1           20
  5 :   wrr , group1           30
  6 :   sp                      0
  7 :   sp                      0
```

Collecting/Clearing Traffic Statistics

Refer to Flow-based Traffic Accounting for information about traffic accounting.

Configuration prerequisites

The ACL rules for traffic classification are defined. Refer to the ACL module of this manual for information about defining ACL rules.

Configuration procedure

You can collect traffic statistics or clear traffic statistics on all the packets matching specific ACL rules, or on packets that match specific ACL rules and are of a VLAN, of a port group, or pass a port.

Follow these steps to collect traffic statistics on all the packets matching specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Collect the statistics on the packets matching specific ACL rules	**traffic-statistic inbound** *acl-rule*	Required
Clear the statistics on the packets matching specific ACL rules	**reset traffic-statistic inbound** *acl-rule*	Optional

Follow these steps to collect traffic statistics on packets that are of a VLAN and match specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Collect the statistics on the packets matching specific ACL rules	**traffic-statistic vlan** *vlan-id* **inbound** *acl-rule*	Required
Clear the statistics on the packets matching specific ACL rules	**reset traffic-statistic vlan** *vlan-id* **inbound** *acl-rule*	Optional

Follow these steps to collect traffic statistics on packets that are of a port group and match specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter port group view	**port-group** *group-id*	—
Collect the statistics on the packets matching specific ACL rules	**traffic-statistic inbound** *acl-rule*	Required
Clear the statistics on the packets matching specific ACL rules	**reset traffic-statistic inbound** *acl-rule*	Optional

Follow these steps to collect traffic statistics on packets passing a port and matching specific ACL rules:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Collect the statistics on the packets matching specific ACL rules	**traffic-statistic inbound** *acl-rule*	Required
Clear the statistics on the packets matching specific ACL rules	**reset traffic-statistic inbound** *acl-rule*	Optional

Caution

As the priority of traffic classification rules is higher than that of the default rules used for processing protocol packets, collecting traffic statistics on all the packets or packets of a VLAN may affect device management that is implemented through Telnet and so on

Configuration example

- GigabitEthernet 1/0/1 is connected to the 10.1.1.0/24 network segment.
- Collect statistics on the packets sourced from the 10.1.1.0/24 network segment.
- Clear the statistics.

1) Method I

```
<device> system-view
```

```
[device] acl number 2000
[device-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[device-acl-basic-2000] quit
[device] interface GigabitEthernet1/0/1
[device-GigabitEthernet1/0/1] traffic-statistic inbound ip-group 2000
[device-GigabitEthernet1/0/1] reset traffic-statistic inbound ip-group 2000
```

2) Method II

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[device-acl-basic-2000] quit
[device] traffic-statistic vlan 2 inbound ip-group 2000
[device] reset traffic-statistic vlan 2 inbound ip-group 2000
```

Enabling the Burst Function

Refer to Burst for information about the burst function.

Configuration prerequisites

The burst function is required.

Configuration procedure

Follow these steps to enable the burst function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the burst function	**burst-mode enable**	Required By default, the burst function is disabled.

Configuration example

Enable the burst function on the devicees.

Configuration procedure:

```
<device> system-view
[device] burst-mode enable
```

Configuring Traffic Mirroring

Refer to Traffic mirroring for information about traffic mirroring.

Configuration prerequisites

- The ACL rules for traffic classification are defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The source mirroring ports and mirroring direction are determined.
- The destination mirroring port is determined.

Configuration procedure

You can configure traffic mirroring on all the packets matching specific ACL rules, or on packets that match specific ACL rules and are of a VLAN, of a port group, or pass a port.

Follow these steps to configure traffic mirroring globally:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view of the destination port	**interface** *interface-type interface-number*	—
Define the current port as the destination port	**monitor-port**	Required
Exit current view	**quit**	—
Reference ACLs for identifying traffic flows and perform traffic mirroring for packets that match.	**mirrored-to inbound** *acl-rule* **monitor-interface**	Required

Follow these steps to configure traffic mirroring for a VLAN:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view of the destination port	**interface** *interface-type interface-number*	—
Define the current port as the destination port	**monitor-port**	Required
Exit current view	**quit**	—
Reference ACLs for identifying traffic flows and perform traffic mirroring for packets that match.	**mirrored-to vlan** *vlan-id* **inbound** *acl-rule* **monitor-interface**	Required

Follow these steps to configure traffic mirroring for a port group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view of the destination port	**interface** *interface-type interface-number*	—
Define the current port as the destination port	**monitor-port**	Required
Exit current view	**quit**	—
Enter port group view	**port-group** *group-id*	—
Reference ACLs for identifying traffic flows and perform traffic mirroring for packets that match.	**mirrored-to inbound** *acl-rule* **monitor-interface**	Required

Follow these steps to configure traffic mirroring for a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view of the destination port	**interface** *interface-type interface-number*	—
Define the current port as the destination port	**monitor-port**	Required
Exit current view	**quit**	—
Enter Ethernet port view of traffic mirroring configuration	**interface** *interface-type interface-number*	—
Reference ACLs for identifying traffic flows and perform traffic mirroring for packets that match.	**mirrored-to inbound** *acl-rule* **monitor-interface**	Required

Caution

As the priority of traffic classification rules is higher than that of the default rules used for processing protocol packets, traffic mirroring on all the packets or packets of a VLAN may affect device management that is implemented through Telnet and so on

Configuration example

Network requirements:

- GigabitEthernet 1/0/1 is connected to the 10.1.1.0/24 network segment.
- Duplicate the packets from network segment 10.1.1.0/24 to the destination mirroring port GigabitEthernet 1/0/4.

1) Method I

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[device-acl-basic-2000] quit
[device] interface GigabitEthernet 1/0/4
[device-GigabitEthernet1/0/4] monitor-port
[device-GigabitEthernet1/0/4] quit
[device] interface GigabitEthernet 1/0/1
[device-GigabitEthernet1/0/1] mirrored-to inbound ip-group 2000 monitor-interface
```

2) Method II

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[device-acl-basic-2000] quit
[device] interface GigabitEthernet 1/0/4
[device-GigabitEthernet1/0/4] monitor-port
[device-GigabitEthernet1/0/4] quit
```

```
[device] mirrored-to vlan 2 inbound ip-group 2000 monitor-interface
```

Displaying and Maintaining QoS

To do…	Use the command…	Remarks
Display the protocol packet priority configuration	**display protocol-priority**	Available in any view
Display the COS-precedence-to-Drop-precedence mapping relationship	**display qos cos-drop-precedence-map**	
Display the COS-precedence-to-DSCP-precedence mapping relationship	**display qos cos-dscp-map**	
Display the COS-precedence-to-local-precedence mapping relationship	**display qos cos-local-precedence-map**	
Display the DSCP-precedence-to-COS-precedence mapping relationship	**display qos dscp-cos-map**	
Display the DSCP-precedence-to-Drop-precedence mapping relationship	**display qos dscp-drop-precedence-map**	
Display the DSCP-precedence-to-DSCP-precedence mapping relationship	**display qos dscp-dscp-map**	
Display the DSCP-precedence-to-local-precedence mapping relationship	**display qos dscp-local-precedence-map**	
Display queue scheduling algorithm and related parameters	**display queue-scheduler**	
Display the QoS-related configuration of a port or all the ports	**display qos-interface** { *interface-type interface-number* | *unit-id* } **all**	
Display the priority trust mode of a port or all the ports	**display qos-interface** { *interface-type interface-number* | *unit-id* } **priority-trust**	
Display traffic shaping configuration of a port or all the ports	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-shape**	
Display traffic policing configuration of a port or all the ports	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-limit**	
Display priority marking configuration of a port or all the ports	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-priority**	
Display traffic redirecting configuration of a port or all the ports	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-redirect**	
Display traffic accounting configuration of a port or all the ports	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-statistic**	

To do…	Use the command…	Remarks
Display VLAN mapping configuration of a port or all the ports	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-remark-vlanid**	
Display traffic mirroring configuration of a port or all the ports	**display qos-interface** { *interface-type interface-number* | *unit-id* } **mirrored-to**	
Display the configuration of traffic mirroring, traffic policing, priority marking, traffic redirecting, or traffic accounting performed for all the packets	**display qos-global** { **all** | **mirrored-to** | **traffic-limit** | **traffic-priority** | **traffic-redirect** | **traffic-statistic** }	
Display the configuration of traffic mirroring, traffic policing, priority marking, traffic redirecting, or traffic accounting performed for packets of a VLAN	**display qos-vlan** [*vlan-id*] { **all** | **mirrored-to** | **traffic-limit** | **traffic-priority** | **traffic-redirect** | **traffic-statistic** }	
Display the configuration of traffic mirroring, traffic policing, priority marking, traffic redirecting, or traffic accounting performed for packets of a port group	**display qos-port-group** [*group-id*] { **all** | **mirrored-to** | **traffic-limit** | **traffic-priority** | **traffic-redirect** | **traffic-statistic** }	

QoS Configuration Example

Configuration Example of Traffic Policing

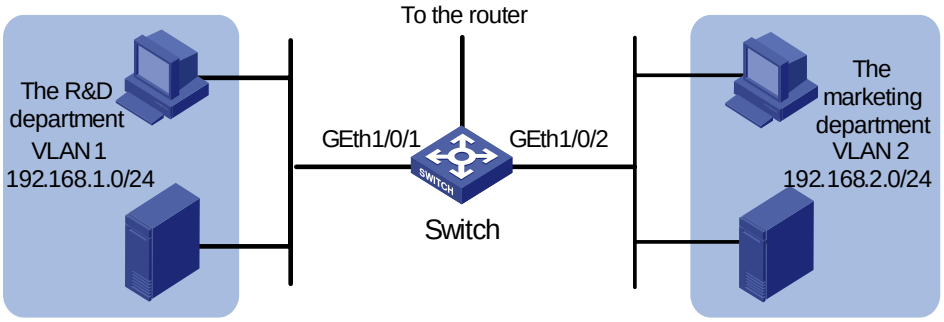
Network requirement

As shown in Figure 1-9, an enterprise network connects all the departments through a device. PC1, with the IP address 192.168.0.1 belongs to the R&D department and is connected to GigabitEthernet 1/0/1 of the switch. The marketing department is connected to GigabitEthernet 1/0/2 of the switch.

Configure traffic policing to satisfy the following requirements:

- Set the maximum rate of outbound IP packets sourced from the marketing department to 64 kbps. Drop the packets exceeding the rate limit.
- Set the maximum rate of outbound IP packets sourced from the R&D department to 128 kbps. Drop the packets exceeding the rate limit.

Figure 1-9 Network diagram for traffic policing and rate limiting configuration



Configuration procedure

1) Define an ACL for traffic classification.

Create ACL 2000 and enter basic ACL view to classify packets sourced from the 192.168.1.0/24 network segment.

```
<device> system-view
[device] acl number 2000
[device-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[device-acl-basic-2000] quit
```

Create ACL 2001 and enter basic ACL view to classify packets sourced from the 192.168.2.0/24 network segment.

```
[device] acl number 2001
[device-acl-basic-2001] rule permit source 192.168.2.0 0.0.0.255
[device-acl-basic-2001] quit
```

2) Configure traffic policing

Set the maximum rate of outbound IP packets sourced from the marketing department to 64 kbps.

```
[device] traffic-limit vlan 2 inbound ip-group 2001 64 exceed drop
```

Set the maximum rate of outbound IP packets sourced from the R&D department to 128 kbps.

```
[device] traffic-limit vlan 1 inbound ip-group 2000 128 exceed drop
```

2 QoS Profile Configuration

Overview

Introduction to QoS Profile

QoS profile is a set of QoS configurations. It provides an easy way for performing and managing QoS configuration. A QoS profile can contain one or multiple QoS functions. In networks where hosts change their positions frequently, you can define QoS policies for the hosts and add the QoS policies to a QoS profile. When a host is connected to another port of a device, you can simply apply the corresponding QoS profile to the port to maintain the same QoS configuration performed for the host.

Currently, a QoS profile can contain configurations concerning packet filtering, traffic policing, and priority marking.

QoS Profile Application Mode

Dynamic application mode

A QoS profile can be applied dynamically to a user or a group of users passing 802.1x authentication. To apply QoS profiles dynamically, a user name-to-QoS profile mapping table is required on the AAA server. For a device operating in this mode, after a user passes the 802.1x authentication, the device looks up the user name-to-QoS profile mapping table for the QoS profile using the user name and then applies the QoS profile found to the port the user is connected to.

Corresponding to the 802.1x authentication modes, dynamic QoS profile application can be user-based and port-based.

- User-based QoS profile application

The device generates a new QoS profile by adding user source MAC address information to the identifying rule defined in the existing QoS profile and then applies the new QoS profile to the port the user is connected to.

- Port-based QoS profile application

The device directly applies the QoS profile to the port the user is connected to.

 **Note**

A user-based QoS profile application fails if the traffic classification rule defined in the QoS profile contains source address information (including source MAC address, source IP address, or both).

Manual application mode

You can use the **apply** command to manually apply a QoS profile to a port.

QoS Profile Configuration

QoS Profile Configuration Task List

Complete the following tasks to configure a QoS profile:

Task	Remarks
Configuring a QoS Profile	Required
Applying a QoS Profile	Optional
Applying a QoS Profile	Optional

Configuring a QoS Profile

Configuration prerequisites

- The ACL rules used for traffic classification are defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The type and number of actions in the QoS profile are specified.

Configuration procedure

Follow these steps to configure a QoS profile:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a QoS profile and enter QoS profile view	**qos-profile** *profile-name*	—
Configure traffic policing	**traffic-limit inbound** *acl-rule target-rate* [**conform** *con-action*] [**exceed** *exceed-action*] [**meter-statistic**]	Optional
Configure packet filtering	**packet-filter inbound** *acl-rule*	Optional Refer to the ACL module of this manual for information about packet filtering.
Configure priority marking	**traffic-priority inbound** *acl-rule* { **dscp** *dscp-value* | **cos** *cos-value* }	Optional

Applying a QoS Profile

You can configure to apply a QoS profile dynamically or simply apply a QoS profile manually.

Configuration prerequisites

- To configure to apply a QoS profile dynamically, make sure 802.1x is enabled both globally and on the port, and the authentication mode is determined. For information about 802.1x, refer to the 802.1x and System Guard module of this manual.
- To apply a QoS profile manually, make sure the port to which the QoS profile is to be applied is determined.
- The QoS profile to be applied is determined.

Configuration procedure

Follow these steps to configure to apply a QoS profile dynamically:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enter Ethernet port view		**interface** *interface-type interface-number*	—
Specify the mode to apply a QoS profile	Configure the mode to apply a QoS profile as port-based	**qos-profile port-based**	Optional By default, the mode to apply a QoS profile is user-based. • If the 802.1x authentication mode is MAC address-based, the mode to apply a QoS profile must be configured user-based. • If the 802.1x authentication mode is port-based, the mode to apply a QoS profile must be configured as port-based.
	Configure the mode to apply a QoS profile as user-based	**undo qos-profile port-based**	

Follow these steps to apply a QoS profile manually:

To do…			Use the command…	Remarks
Enter system view			**system-view**	**—**
Apply a QoS profile to specific ports	In system view		**apply qos-profile** *profile-name* **interface** *interface-list*	Select either of the operations. By default, a port has no QoS profile applied to it.
	In Ethernet port view	Enter Ethernet port view	**interface** *interface-type interface-number*	
		Apply a QoS profile to the current port	**apply qos-profile** *profile-name*	

Displaying and Maintaining QoS Profile

To do…	Use the command…	Remarks
Display QoS profile configuration	**display qos-profile** { **all** | **name** *profile-name* | **interface** *interface-type interface-number* | **user** *user-name* }	Available in any view

Configuration Example

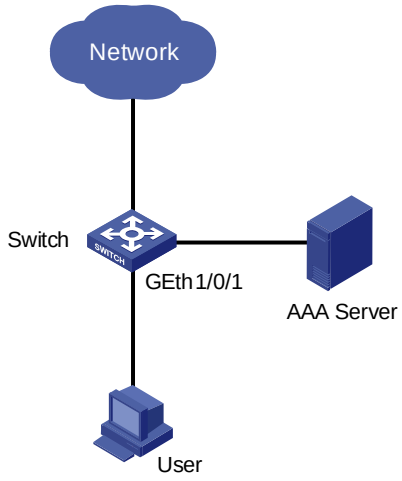
QoS Profile Configuration Example

Network requirements

As shown in Figure 2-1, the user name is “someone”, and the authentication password is “hello”. It is connected to GigabitEthernet 1/0/1 of the switch and belongs to the test.net domain.

It is required to configure a QoS profile to limit the rate of all the outbound IP packets of the user to 128 kbps and configuring to drop the packets exceeding the target packet rate.

Figure 2-1 Network diagram for QoS profile configuration



Configuration procedure

1) Configuration on the AAA server

Configure the user authentication information and the matching relationship between the user name and the QoS profile. Refer to the user manual of the AAA server for detailed configuration.

2) Configuration on the switch

Configure IP addresses for the RADIUS server.

```
<device> system-view
[device] radius scheme radius1
[device-radius-radius1] primary authentication 10.11.1.1
[device-radius-radius1] primary accounting 10.11.1.2
[device-radius-radius1] secondary authentication 10.11.1.2
[device-radius-radius1] secondary accounting 10.11.1.1
```

Set the encryption passwords for the device to exchange packets with the authentication RADIUS servers and accounting RADIUS servers.

```
[device-radius-radius1] key authentication money
[device-radius-radius1] key accounting money
```

Configure the device to delete the user domain name from the user name and then send the user name to the RADIUS sever.

```
[device-radius-radius1] user-name-format without-domain
[device-radius-radius1] quit
```

Create the user domain test.net and specify radius1 as your RADIUS server group.

```
[device] domain test.net
[device-isp-test.net] radius-scheme radius1
[device-isp-test.net] quit
```

Create ACL 3000 to permit IP packets destined for any IP address.

```
[device] acl number 3000
[device-acl-adv-3000] rule 1 permit ip destination any
[device-acl-adv-3000] quit
```

Define a QoS profile named “example” to limit the rate of matched packets to 128 kbps and configuring to drop the packets exceeding the target packet rate.

```
[device] qos-profile example
[device-qos-profile-example] traffic-limit inbound ip-group 3000 128 exceed drop
```

Enable 802.1x.

```
[device] dot1x
[device] dot1x interface GigabitEthernet1/0/1
```

After the configuration, the QoS profile named “example” will be applied to the user with user name “someone” automatically after the user passes the authentication.

Table of Contents

1 Mirroring Configuration ····· 1-1
Mirroring Overview ····· 1-1
Local Port Mirroring ····· 1-2
Remote Port Mirroring ····· 1-2
MAC-Based Mirroring ····· 1-3
VLAN-Based Mirroring ····· 1-3
Mirroring Configuration ····· 1-4
Configuring Local Port Mirroring ····· 1-4
Configuring Remote Port Mirroring ····· 1-5
Configuring MAC-Based Mirroring ····· 1-7
Configuring VLAN-Based Mirroring ····· 1-8
Displaying and Maintaining Port Mirroring ····· 1-9
Mirroring Configuration Example ····· 1-9
Local Port Mirroring Configuration Example ····· 1-9
Remote Port Mirroring Configuration Example ····· 1-10

1 Mirroring Configuration

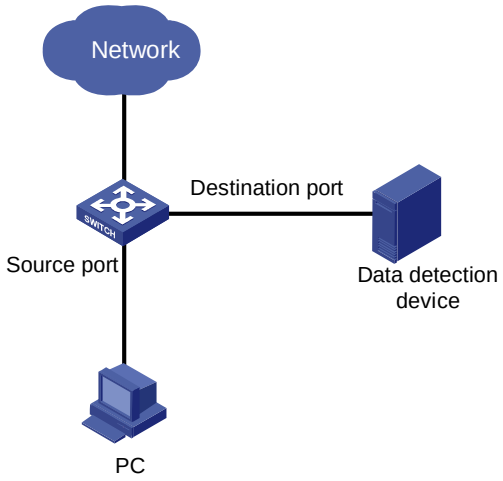
Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Mirroring Overview

Mirroring refers to the process of copying packets of one or more ports (source ports) to a destination port which is connected to a data detection device. Users can then use the data detection device to analyze the mirrored packets on the destination port for monitoring and troubleshooting the network.

Figure 1-1 Mirroring



The device supports four kinds of port mirroring:

- Local port mirroring: a device copies packets passing through one or more source ports of the device to the destination port.
- Remote port mirroring implements port mirroring through the remote source mirroring group and remote destination mirroring group. The device copies the packets of the source port to the reflector port, which then broadcasts the packets in the remote-probe VLAN. After the remote device receives the packets, it compares the VLAN ID of the packets with that of the remote-probe VLAN on the remote device. If the VLAN IDs are identical, the remote device forwards the packets to the destination port of the remote destination mirroring group.
- MAC-based mirroring: a device copies packets matching a specified MAC address to the destination port.

- VLAN-based mirroring: a device copies packets of a specified VLAN to the destination port.

Local Port Mirroring

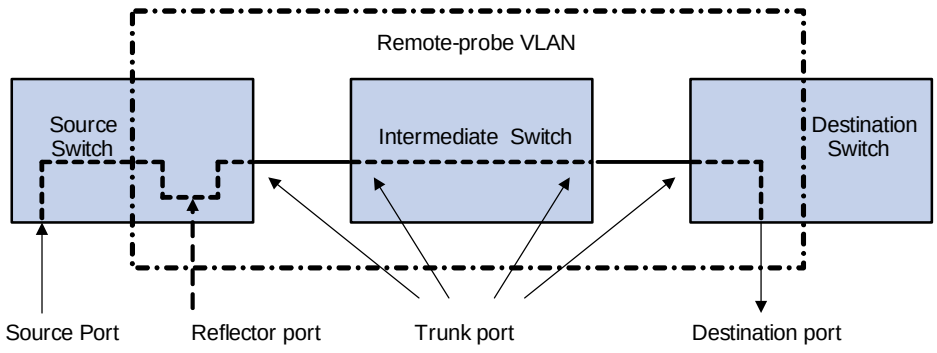
In local port mirroring, packets passing through one or more source ports of a device are copied to the destination port on the same device for packet analysis and monitoring. In this case, the source ports and the destination port must be located on the same device.

Remote Port Mirroring

Remote port mirroring does not require the source and destination ports to be on the same device. The source and destination ports can be located on multiple devices across the network. Therefore, administrators can monitor the traffic on remote devices conveniently.

To implement remote port mirroring, a special VLAN, called remote-probe VLAN, is needed. All mirrored packets are sent from the reflector port of the source switch to the monitor port (destination port) of the destination switch through the remote-probe VLAN, so as to implement the monitoring of packets received on and sent from the source switch on the destination switch. Figure 1-2 illustrates the implementation of remote port mirroring.

Figure 1-2 Remote port mirroring application



The switches involved in the remote port mirroring implementation play the following three roles.

- Source switch: The monitored port resident switch. It copies traffic to the reflector port, which then transmits the traffic to an intermediate switch or destination switch through the remote-probe VLAN.
- Intermediate switch: Switches between the source switch and destination switch on the network. An intermediate switch forwards mirrored traffic flows to the next intermediate switch or the destination switch through the remote-probe VLAN. No intermediate switch is present if the source and destination switches directly connect to each other.
- Destination switch: The remote mirroring destination port resident switch. It forwards mirrored traffic flows it received from the remote-probe VLAN to the monitoring device through the destination port.

Table 1-1 describes how the ports on various switches are involved in the mirroring operation.

Table 1-1 Ports involved in the mirroring operation

Switch	Ports involved	Function
Source switch	Source port	Port monitored. It copies packets to the reflector port through local port mirroring. There can be more than one source port.
	Reflector port	Receives packets from the source port and broadcasts the packets in the remote-probe VLAN.
	Trunk port	Sends mirrored packets to the intermediate switch or the destination switch.
Intermediate switch	Trunk port	Sends mirrored packets to the destination switch. Two trunk ports are necessary for the intermediate switch to connect the devices at the source switch side and the destination switch side.
Destination switch	Trunk port	Receives remote mirrored packets.
	Destination port	Receives packets forwarded from the trunk port and transmits the packets to the data detection device.

Caution

- Do not configure a default VLAN, a management VLAN, or a dynamic VLAN as the remote-probe VLAN.
- Configure all ports connecting the devices in the remote-probe VLAN as trunk ports, and ensure the Layer 2 connectivity from the source switch to the destination switch over the remote-probe VLAN.
- Do not configure a Layer 3 interface for the remote-probe VLAN, run other protocol packets, or carry other service packets on the remote-prove VLAN and do not use the remote-prove VLAN as the voice VLAN and protocol VLAN; otherwise, remote port mirroring may be affected.

MAC-Based Mirroring

With MAC-based mirroring configured, a device mirrors packets matching the specified MAC address to the destination port, including:

- Packets with the source MAC address matching the specified MAC address.
- Packets with the destination MAC address matching the specified MAC address.

Compared with port mirroring, MAC-based mirroring is more precise and it can be used to monitor packets of specific device in the network.

VLAN-Based Mirroring

With VLAN-based mirroring configured, a device mirrors packets received on all ports in the specified VLAN to the destination port.

Compared with port mirroring, VLAN-based mirroring is more extensive and it can be used to monitor packets of a specific VLAN or VLANs in the network.

Mirroring Configuration

Complete the following tasks to configure mirroring:

Task	Remarks
Configuring Local Port Mirroring	Optional
Configuring Remote Port Mirroring	Optional
Configuring MAC-Based Mirroring	Optional
Configuring VLAN-Based Mirroring	Optional

Configuring Local Port Mirroring

Configuration prerequisites

- The source port is determined and the direction in which the packets are to be mirrored is determined.
- The destination port is determined.

Configuration procedure

Follow these steps to configure local port mirroring:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Create a port mirroring group		**mirroring-group** *group-id* **local**	Required
Configure the source port for the port mirroring group	In system view	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	Use either approach You can configure multiple source ports at a time in system view, or you can configure the source port in specific port view. The configurations in the two views have the same effect.
	In port view	**interface** *interface-type interface-number*	
		mirroring-group *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }	
		quit	
Configure the destination port for the port mirroring group	In system view	**mirroring-group** *group-id* **monitor-port** *monitor-port-id*	Use either approach The configurations in the two views have the same effect.
	In port view	**interface** *interface-type interface-number*	
		mirroring-group *group-id* **monitor-port**	

When configuring local port mirroring, note that:

- You need to configure the source and destination ports for the local port mirroring to take effect.
- The source port and the destination port cannot be a member port of an existing mirroring group; besides, the destination port cannot be a member port of an aggregation group or a port enabled with LACP or STP.

Configuring Remote Port Mirroring

Note

The device can serve as a source switch, an intermediate switch, or a destination switch in a remote port mirroring networking environment.

Configuration on the device acting as a source switch

1) Configuration prerequisites

- The source port, the reflector port, and the remote-probe VLAN are determined.
- Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.
- The direction of the packets to be monitored is determined.

2) Configuration procedure

Follow these steps to configure the source switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a VLAN and enter the VLAN view	**vlan** *vlan-id*	*vlan-id* is the ID of the remote-probe VLAN.
Configure the current VLAN as the remote-probe VLAN	**remote-probe vlan enable**	Required
Return to system view	**quit**	—
Enter the view of the Ethernet port that connects to the intermediate switch or destination switch	**interface** *interface-type interface-number*	—
Configure the current port as trunk port	**port link-type trunk**	Required By default, the port type is Access.
Configure the trunk port to permit packets from the remote-probe VLAN	**port trunk permit vlan** *remote-probe-vlan-id*	Required
Return to system view	**quit**	—
Create a remote source mirroring group	**mirroring-group** *group-id* **remote-source**	Required
Configure source port(s) for the remote source mirroring group	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	Required
Configure the reflector port for the remote source mirroring group	**mirroring-group** *group-id* **reflector-port** *reflector-port*	Required
Configure the remote-probe VLAN for the remote source mirroring group	**mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*	Required

When configuring the source switch, note that:

- All ports of a remote source mirroring group are on the same device. Each remote source mirroring group can be configured with only one reflector port.
- The reflector port cannot be a member port of an existing mirroring group, a member port of an aggregation group, or a port enabled with LACP or STP. It must be an access port and cannot be configured with the functions like VLAN-VPN, port loopback detection, QoS, port security, and so on.
- You cannot modify the duplex mode, port rate, and MDI attribute of a reflector port.
- Only an existing static VLAN can be configured as the remote-probe VLAN. To remove a remote-probe VLAN, you need to restore it to a normal VLAN first. A remote port mirroring group gets invalid if the corresponding remote port mirroring VLAN is removed.
- Do not configure a port connecting the intermediate switch or destination switch as the mirroring source port. Otherwise, traffic disorder may occur in the network.

Configuration on the device acting as an intermediate switch

1) Configuration prerequisites

- The trunk ports and the remote-probe VLAN are determined.
- Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.

2) Configuration procedure

Follow these steps to configure the intermediate switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	v*lan-id* is the ID of the remote-probe VLAN.
Configure the current VLAN as the remote-probe VLAN	**remote-probe vlan enable**	Required
Return to system view	**quit**	—
Enter the view of the Ethernet port connecting to the source switch, destination switch or other intermediate switch	**interface** *interface-type interface-number*	—
Configure the current port as trunk port	**port link-type trunk**	Required By default, the port type is Access.
Configure the trunk port to permit packets from the remote-probe VLAN	**port trunk permit vlan** *remote-probe-vlan-id*	Required

Configuration on the device acting as a destination switch

1) Configuration prerequisites

- The destination port and the remote-probe VLAN are determined.
- Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.

2) Configuration procedure

Follow these steps to configure remote port mirroring on the destination switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	v*lan-id* is the ID of the remote-probe VLAN.
Configure the current VLAN as a remote-probe VLAN	**remote-probe vlan enable**	Required
Return to system view	**quit**	—
Enter the view of the Ethernet port connecting to the source switch or an intermediate switch	**interface** *interface-type interface-number*	—
Configure the current port as trunk port	**port link-type trunk**	Required By default, the port type is Access.
Configure trunk port to permit packets from the remote-probe VLAN	**port trunk permit vlan** *remote*-probe-*vlan-id*	Required
Return to system view	**quit**	—
Create a remote destination mirroring group	**mirroring-group** *group-id* **remote-destination**	Required
Configure the destination port for the remote destination mirroring group	**mirroring-group** *group-id* **monitor-port** *monitor-port*	Required
Configure the remote-probe VLAN for the remote destination mirroring group	**mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*	Required

When configuring a destination switch, note that:

- The destination port of remote port mirroring cannot be a member port of an existing mirroring group, a member port of an aggregation group, or a port enabled with LACP or STP.
- Only an existing static VLAN can be configured as the remote-probe VLAN. To remove a remote-probe VLAN, you need to restore it to a normal VLAN first. A remote port mirroring group gets invalid if the corresponding remote port mirroring VLAN is removed.

Configuring MAC-Based Mirroring

Note

- The MAC address specified for MAC-based mirroring must be a static MAC address existing in the MAC address table.
- You can configure MAC-based mirroring for a remote source mirroring group to implement the MAC-based remote mirroring function.

Configuration prerequisites

- The MAC address to be matched is determined.
- The destination port is determined.

Configuration procedure

Follow these steps to configure MAC-based mirroring:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a local or remote source mirroring group	**mirroring-group** *group-id* { **local** | **remote-source** }	Required
Configuring MAC-Based Mirroring	**mirroring-group** *group-id* **mirroring-mac** *mac* **vlan** *vlan-id*	Required
Configure the destination port for the mirroring group	**mirroring-group** *group-id* **monitor-port** *monitor-port-id*	Required Note that you need not configure the destination port on the source switch when configuring MAC-based remote mirroring.

Configuration example

Configure MAC-based mirroring to mirror packets whose source/destination MAC addresses match 000f-e20f-0101 to port GigabitEthernet 1/0/2 on the local device.

Configuration procedure:

```
<device> system-view
[device] mac-address static 000f-e20f-0101 interface Gigabitethernet 1/0/1 vlan 2
[device] mirroring-group 1 local
[device] mirroring-group 1 mirroring-mac 000f-e20f-0101 vlan 2
[device] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
```

Configuring VLAN-Based Mirroring

Note

You can configure VLAN-based mirroring for a remote source mirroring group to implement the VLAN-based remote mirroring function.

Configuration prerequisites

- The VLAN to be monitored is determined.
- The destination port is determined.

Configuration procedure

Follow these steps to configure VLAN-based mirroring:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a local or remote source mirroring group	**mirroring-group** *group-id* { **local** | **remote-source** }	Required
Configuring VLAN-Based Mirroring	**mirroring-group** *group-id* **mirroring-vlan** *vlan-id* **inbound**	Required
Configure the destination port for the mirroring group	**mirroring-group** *group-id* **monitor-port** *monitor-port-id*	Required Note that you need not configure the destination port on the source switch when configuring VLAN-based remote mirroring.

Configuration example

Configure VLAN-based mirroring to mirror packets received on all ports in VLAN 2 to port GigabitEthernet 1/0/2 on the local device.

Configuration procedure:

```
<device> system-view
[device] mirroring-group 1 local
[device] mirroring-group 1 mirroring-vlan 2 inbound
[device] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
```

Displaying and Maintaining Port Mirroring

To do…	Use the command…	Remarks
Display the information of a mirroring group.	**display mirroring-group** { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }	Available in any view

Mirroring Configuration Example

Local Port Mirroring Configuration Example

Network requirements

The departments of a company connect to each other through switches, as shown in Figure 1-3:

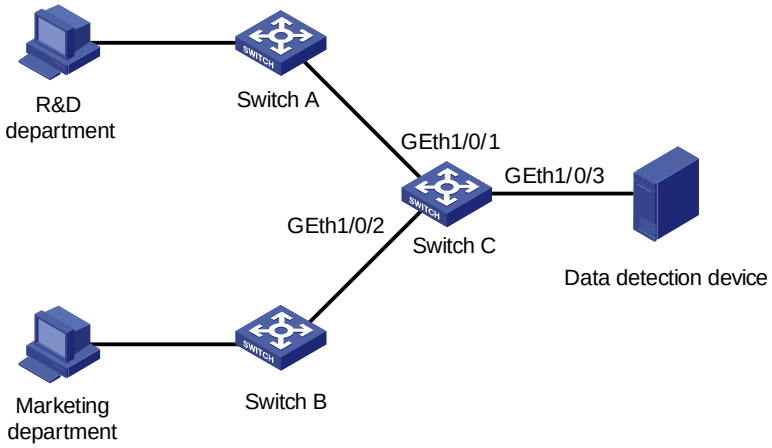
- Research and Development (R&D) department is connected to Switch C through GigabitEthernet 1/0/1.
- Marketing department is connected to Switch C through GigabitEthernet 1/0/2.
- Data detection device is connected to Switch C through GigabitEthernet 1/0/3

The administrator wants to monitor the packets received on and sent from the R&D department and the marketing department through the data detection device.

Use the local port mirroring function to meet the requirement. Perform the following configurations on Switch C.

- Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as mirroring source ports.
- Configure GigabitEthernet 1/0/3 as the mirroring destination port.

Figure 1-3 Network diagram for local port mirroring



Configuration procedure

Configure Switch C:

Create a local mirroring group.

```
<device> system-view
[device] mirroring-group 1 local
```

Configure the source ports and destination port for the local mirroring group.

```
[device] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2 both
[device] mirroring-group 1 monitor-port GigabitEthernet 1/0/3
```

Display configuration information about local mirroring group 1.

```
[device] display mirroring-group 1
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/1  both
        GigabitEthernet1/0/2  both
    mirroring mac:
    mirroring vlan:
    monitor port: GigabitEthernet1/0/3
```

After the configurations, you can monitor all packets received on and sent from the R&D department and the marketing department on the data detection device.

Remote Port Mirroring Configuration Example

Network requirements

The departments of a company connect to each other through switches, as shown in Figure 1-4:

- Switch A, Switch B, and Switch C are WX3000 series devices.

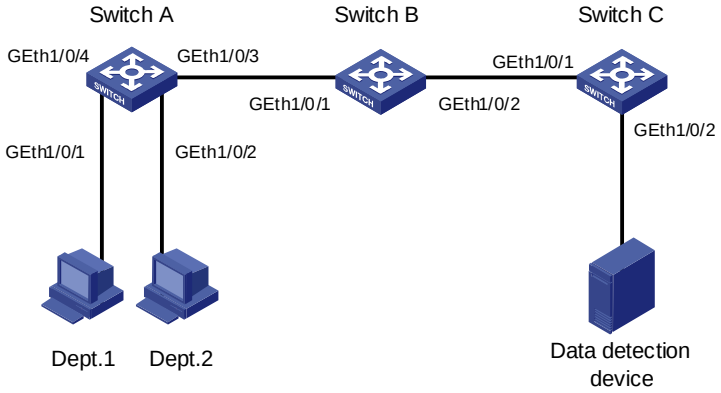
- Department 1 is connected to GigabitEthernet 1/0/1 of Switch A.
- Department 2 is connected to GigabitEthernet 1/0/2 of Switch A.
- GigabitEthernet 1/0/3 of Switch A connects to GigabitEthernet 1/0/1 of Switch B.
- GigabitEthernet 1/0/2 of Switch B connects to GigabitEthernet 1/0/1 of Switch C.
- The data detection device is connected to GigabitEthernet 1/0/2 of Switch C.

The administrator wants to monitor the packets sent from Department 1 and 2 through the data detection device.

Use the remote port mirroring function to meet the requirement. Perform the following configurations:

- Use Switch A as the source switch, Switch B as the intermediate switch, and Switch C as the destination switch.
- On Switch A, create a remote source mirroring group, configure VLAN 10 as the remote-probe VLAN, ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as the source ports, and port GigabitEthernet 1/0/4 as the reflector port.
- On Switch B, configure VLAN 10 as the remote-probe VLAN.
- Configure GigabitEthernet 1/0/3 of Switch A, GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch B, and GigabitEthernet 1/0/1 of Switch C as trunk ports, allowing packets of VLAN 10 to pass.
- On Switch C, create a remote destination mirroring group, configure VLAN 10 as the remote-probe VLAN, and configure GigabitEthernet 1/0/2 connected with the data detection device as the destination port.

Figure 1-4 Network diagram for remote port mirroring



Configuration procedure

1) Configure the source switch (Switch A)

Create remote source mirroring group 1.

```
<device> system-view
[device] mirroring-group 1 remote-source
```

Configure VLAN 10 as the remote-probe VLAN.

```
[device] vlan 10
[device-vlan10] remote-probe vlan enable
[device-vlan10] quit
```

Configure the source ports, reflector port, and remote-probe VLAN for the remote source mirroring group.

```
[device] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2
inbound
[device] mirroring-group 1 reflector-port GigabitEthernet 1/0/4
[device] mirroring-group 1 remote-probe vlan 10
```

Configure GigabitEthernet 1/0/3 as trunk port, allowing packets of VLAN 10 to pass.

```
[device] interface GigabitEthernet 1/0/3
[device-GigabitEthernet1/0/3] port link-type trunk
[device-GigabitEthernet1/0/3] port trunk permit vlan 10
[device-GigabitEthernet1/0/3] quit
```

Display configuration information about remote source mirroring group 1.

```
[device] display mirroring-group 1
mirroring-group 1:
    type: remote-source
    status: active
    mirroring port:
        GigabitEthernet1/0/1  inbound
        GigabitEthernet1/0/2  inbound
    mirroring mac:
    mirroring vlan:
    reflector port: GigabitEthernet1/0/4
    remote-probe vlan: 10
```

2) Configure the intermediate switch (Switch B)

Configure VLAN 10 as the remote-probe VLAN.

```
<device> system-view
[device] vlan 10
[device-vlan10] remote-probe vlan enable
[device-vlan10] quit
```

Configure GigabitEthernet 1/0/1 as the trunk port, allowing packets of VLAN 10 to pass.

```
[device] interface GigabitEthernet 1/0/1
[device-GigabitEthernet1/0/1] port link-type trunk
[device-GigabitEthernet1/0/1] port trunk permit vlan 10
[device-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as the trunk port, allowing packets of VLAN 10 to pass.

```
[device] interface GigabitEthernet 1/0/2
[device-GigabitEthernet1/0/2] port link-type trunk
[device-GigabitEthernet1/0/2] port trunk permit vlan 10
```

3) Configure the destination switch (Switch C)

Create remote destination mirroring group 1.

```
<device> system-view
[device] mirroring-group 1 remote-destination
```

Configure VLAN 10 as the remote-probe VLAN.

```
[device] vlan 10
[device-vlan10] remote-probe vlan enable
[device-vlan10] quit
```

Configure the destination port and remote-probe VLAN for the remote destination mirroring group.

```
[device] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
[device] mirroring-group 1 remote-probe vlan 10
```

Configure GigabitEthernet 1/0/1 as the trunk port, allowing packets of VLAN 10 to pass.

```
[device] interface GigabitEthernet 1/0/1
[device-GigabitEthernet1/0/1] port link-type trunk
[device-GigabitEthernet1/0/1] port trunk permit vlan 10
[device-GigabitEthernet1/0/1] quit
```

Display configuration information about remote destination mirroring group 1.

```
[device] display mirroring-group 1
mirroring-group 1:
    type: remote-destination
    status: active
    monitor port: GigabitEthernet1/0/2
    remote-probe vlan: 10
```

After the configurations, you can monitor all packets sent from Department 1 and 2 on the data detection device.

Table of Contents

1 ARP Configuration 1-1
Introduction to ARP 1-1
ARP Function 1-1
ARP Message Format 1-1
ARP Table 1-3
ARP Process 1-3
Introduction to ARP Attack Detection 1-4
Introduction to Gratuitous ARP 1-5
Configuring ARP 1-5
Configuring ARP Basic Functions 1-5
Configuring ARP Attack Detection 1-6
Configuring Gratuitous ARP 1-7
Displaying and Maintaining ARP 1-8
ARP Configuration Example 1-8
ARP Basic Configuration Example 1-8
ARP Attack Detection Configuration Example 1-8

1 ARP Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Introduction to ARP

ARP Function

Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address.

An IP address is the address of a host at the network layer. To send a network layer packet to a destination host, the device must know the data link layer address (MAC address, for example) of the destination host or the next hop. To this end, the IP address must be resolved into the corresponding data link layer address.

Note

Unless otherwise stated, a data link layer address in this chapter refers to a 48-bit Ethernet MAC address.

ARP Message Format

ARP messages are classified as ARP request messages and ARP reply messages. Figure 1-1 illustrates the format of these two types of ARP messages.

- As for an ARP request, all the fields except the hardware address of the receiver field are set. The hardware address of the receiver is what the sender requests for.
- As for an ARP reply, all the fields are set.

Figure 1-1 ARP message format

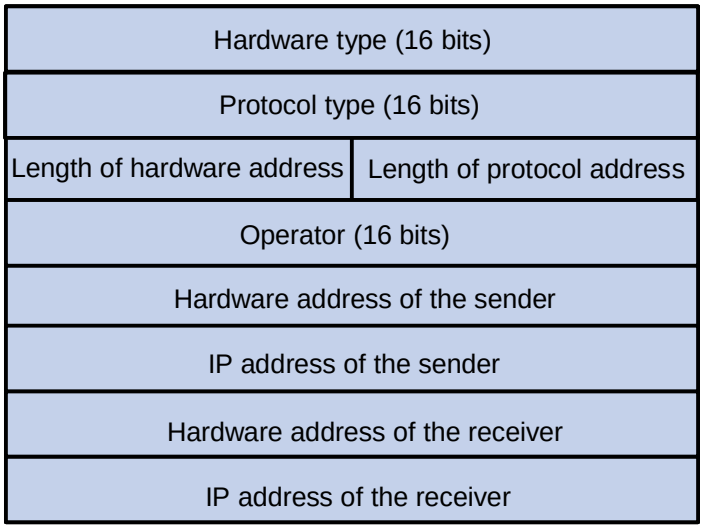


Table 1-1 describes the fields of an ARP packet.

Table 1-1 Description on the fields of an ARP packet

Field	Description
Hardware Type	Type of the hardware interface. Refer to Table 1-2 for the information about the field values.
Protocol type	Type of protocol address to be mapped. 0x0800 indicates an IP address.
Length of hardware address	Hardware address length (in bytes)
Length of protocol address	Protocol address length (in bytes)
Operator	Indicates the type of a data packets, which can be: • 1: ARP request packets • 2: ARP reply packets • 3: RARP request packets • 4: RARP reply packets
Hardware address of the sender	Hardware address of the sender
IP address of the sender	IP address of the sender
Hardware address of the receiver	• For an ARP request packet, this field is null. • For an ARP reply packet, this field carries the hardware address of the receiver.
IP address of the receiver	IP address of the receiver

Table 1-2 Description on the values of the hardware type field

Value	Description
1	Ethernet
2	Experimental Ethernet
3	X.25
4	Proteon ProNET (Token Ring)

Value	Description
5	Chaos
6	IEEE802.X
7	ARC network

ARP Table

In an Ethernet, the MAC addresses of two hosts must be available for the two hosts to communicate with each other. Each host in an Ethernet maintains an ARP table, where the latest used IP address-to-MAC address mapping entries are stored. The device provides the **display arp** command to display the information about ARP mapping entries.

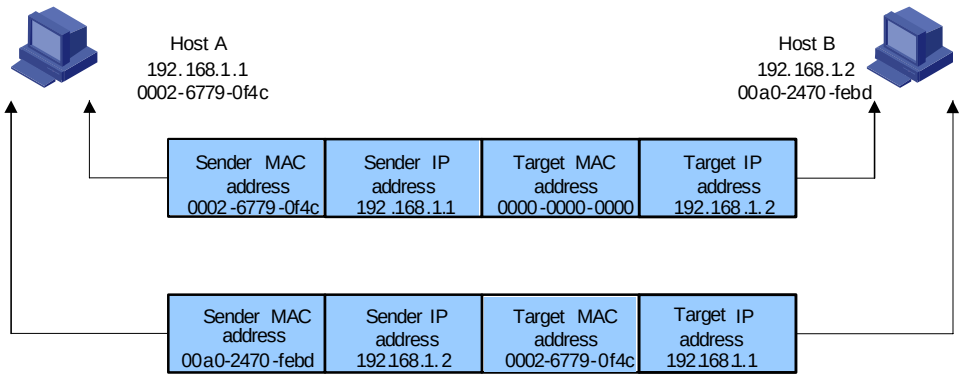
ARP entries in a device can either be static entries or dynamic entries, as described in Table 1-3.

Table 1-3 ARP entries

ARP entry	Generation Method	Maintenance Mode
Static ARP entry	Manually configured	Manual maintenance
Dynamic ARP entry	Dynamically generated	ARP entries of this type age with time. The aging period is set by the ARP aging timer.

ARP Process

Figure 1-2 ARP process



Suppose that Host A and Host B are on the same subnet and that Host A sends a message to Host B. The resolution process is as follows:

2) Host A looks in its ARP mapping table to see whether there is an ARP entry for Host B. If Host A finds it, Host A uses the MAC address in the entry to encapsulate the IP packet into a data link layer frame and sends the frame to Host B.
3) If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request, in which the source IP address and source MAC address are respectively the IP address and MAC address of Host A and the destination IP address and MAC address are respectively the IP address of Host B and an all-zero MAC address. Because the ARP request is sent in broadcast

mode, all hosts on this subnet can receive the request, but only the requested host (namely, Host B) will process the request.

4) Host B compares its own IP address with the destination IP address in the ARP request. If they are the same, Host B saves the source IP address and source MAC address into its ARP mapping table, encapsulates its MAC address into an ARP reply, and unicasts the reply to Host A.
5) After receiving the ARP reply, Host A adds the MAC address of Host B into its ARP mapping table for subsequent packet forwarding. Meanwhile, Host A encapsulates the IP packet and sends it out.

Usually ARP dynamically implements and automatically seeks mappings from IP addresses to MAC addresses, without manual intervention.

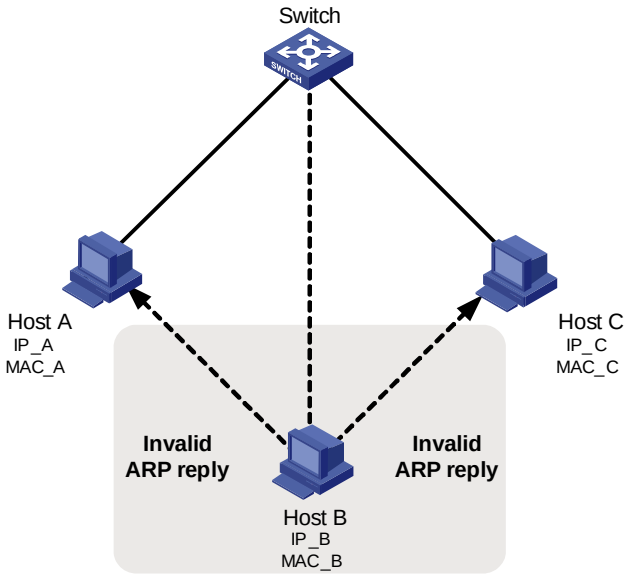
Introduction to ARP Attack Detection

Man-in-the-middle attack

According to the ARP design, after receiving an ARP response, a host adds the IP-to-MAC mapping of the sender into its ARP mapping table even if the MAC address is not the real one. This can reduce the ARP traffic in the network, but it also makes ARP spoofing possible.

In Figure 1-3, Host A communicates with Host C through Switch. To intercept the traffic between Host A and Host C, the hacker (Host B) forwards invalid ARP reply messages to Host A and Host C respectively, causing the two hosts to update the MAC address corresponding to the peer IP address in their ARP tables with the MAC address of Host B. Then, the traffic between Host A and C will pass through Host B which acts like a “man-in-the-middle” that may intercept and modify the communication information. Such attack is called man-in-the-middle attack.

Figure 1-3 Network diagram for ARP man-in-the-middle attack



ARP attack detection

To guard against the man-in-the-middle attacks launched by hackers or attackers, the device supports the ARP attack detection function. All ARP (both request and response) packets passing through the device are redirected to the CPU, which checks the validity of all the ARP packets by using the DHCP snooping table or the manually configured IP binding table. For description of DHCP snooping table and the manually configured IP binding table, refer to the DHCP snooping section in the part discussing DHCP in this manual.

After you enable the ARP attack detection function, the device will check the following items of an ARP packet: the source MAC address, source IP address, port number of the port receiving the ARP packet, and the ID of the VLAN the port resides. If these items match the entries of the DHCP snooping table or the manual configured IP binding table, the device will forward the ARP packet; if not, the device discards the ARP packet.

- With trusted ports configured, ARP packets coming from the trusted ports will not be checked, while those from other ports will be checked through the DHCP snooping table or the manually configured IP binding table.
- With the ARP restricted forwarding function enabled, ARP request packets are forwarded through trusted ports only; ARP response packets are forwarded according to the MAC addresses in the packets, or through trusted ports if the MAC address table contains no such destination MAC addresses.

Introduction to Gratuitous ARP

The following are the characteristics of gratuitous ARP packets:

- Both source and destination IP addresses carried in a gratuitous ARP packet are the local addresses, and the source MAC address carried in it is the local MAC addresses.
- If a device finds that the IP addresses carried in a received gratuitous packet conflict with those of its own, it returns an ARP response to the sending device to notify of the IP address conflict.

By sending gratuitous ARP packets, a network device can:

- Determine whether or not IP address conflicts exist between it and other network devices.
- Trigger other network devices to update its hardware address stored in their caches.

The gratuitous ARP packet learning function:

When the gratuitous ARP packet learning function is enabled on a device and the device receives a gratuitous ARP packet, the device updates the existing ARP entry (contained in the cache of the device) that matches the received gratuitous ARP packet using the hardware address of the sender carried in the gratuitous ARP packet.

Configuring ARP

Configuring ARP Basic Functions

Follow these steps to configure ARP basic functions:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Add a static ARP entry	**arp static** *ip-address mac-address* [*vlan-id interface-type interface-number*]	Optional By default, the ARP mapping table is empty, and the address mapping entries are created dynamically by ARP.
Configure the ARP aging timer	**arp timer aging** *aging-time*	Optional By default, the ARP aging timer is set to 20 minutes.

To do…	Use the command…	Remarks
Enable the ARP entry checking function (that is, disable the device from learning ARP entries with multicast MAC addresses)	**arp check enable**	Optional By default, the ARP entry checking function is enabled.

Caution

- Static ARP entries are valid as long as the device operates normally. But some operations, such as removing a VLAN, or removing a port from a VLAN, will make the corresponding ARP entries invalid and therefore removed automatically.
- As for the **arp static** command, the value of the *vlan-id* argument must be the ID of an existing VLAN, and the port identified by the *interface-type* and *interface-number* arguments must belong to the VLAN.
- Currently, static ARP entries cannot be configured on the ports of an aggregation group.

Configuring ARP Attack Detection

Follow these steps to configure the ARP attack detection function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable DHCP snooping	**dhcp-snooping**	Required By default, the DHCP snooping function is disabled.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Specify the current port as a trusted port	**dhcp-snooping trust**	Required By default, after DHCP snooping is enabled, all ports of a device are untrusted ports.
Quit to system view	**quit**	—
Enter VLAN view	**vlan** *vlan-id*	—
Enable the ARP attack detection function	**arp detection enable**	Required By default, ARP attack detection is disabled on all ports.
Quit to system view	**quit**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the port as an ARP trusted port	**arp detection trust**	Optional By default, a port is an untrusted port.

To do…	Use the command…	Remarks
Quit to system view	**quit**	—
Enter VLAN view	**vlan** *vlan-id*	—
Enable ARP restricted forwarding	**arp restricted-forwarding enable**	Optional By default, the ARP restricted forwarding function is disabled. The device forwards legal ARP packets through all its ports.

Note

- You need to enable DHCP snooping and configure DHCP snooping trusted ports on the device before configuring the ARP attack detection function. For more information about DHCP snooping, refer to the DHCP snooping section in the part discussing DHCP in this manual.
- Generally, the uplink port of a device is configured as a trusted port.
- Before enabling ARP restricted forwarding, make sure you enable ARP attack detection and configure ARP trusted ports.
- You are not recommended to configure ARP attack detection on the ports of an aggregation group.

Configuring Gratuitous ARP

Follow these steps to configure the gratuitous ARP:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the gratuitous ARP packet learning function	**gratuitous-arp-learning enable**	Optional By default, the gratuitous ARP packet learning function is enabled.

Note

The sending of gratuitous ARP packets is enabled as long as a device operates. No command is needed for enabling this function. That is, the device sends gratuitous ARP packets whenever a VLAN interface is enabled (such as when a link is enabled or an IP address is configured for the VLAN interface) or whenever the IP address of a VLAN interface is changed.

Displaying and Maintaining ARP

To do…	Use the command…	Remarks
Display specific ARP mapping table entries	**display arp** [**static** | **dynamic** | *ip-address*]	Available in any view
Display the ARP mapping entries related to a specified string in a specified way	**display arp** [**dynamic** | **static**] | { **begin** | **include** | **exclude** } *text*	
Display the number of the ARP entries of a specified type	**display arp count** [[**dynamic** | **static**] [| { **begin** | **include** | **exclude** } *text*] | *ip-address*]	
Display the statistics about the untrusted ARP packets dropped by the specified port	**display arp detection statistics interface** *interface-type interface-number*	
Display the setting of the ARP aging timer	**display arp timer aging**	
Clear specific ARP entries	**reset arp** [**dynamic** | **static** | **interface** *interface-type interface-number*]	Available in user view

ARP Configuration Example

ARP Basic Configuration Example

Network requirement

- Disable ARP entry check on the device.
- Set the aging time for dynamic ARP entries to 10 minutes.
- Add a static ARP entry, with the IP address being 192.168.1.1, the MAC address being 000f-e201-0000, and the outbound port being GigabitEthernet 1/0/10 of VLAN 1.

Configuration procedure

```
<device> system-view
[device] undo arp check enable
[device] arp timer aging 10
[device] arp static 192.168.1.1 000f-e201-0000 1 gigabitethernet 1/0/10
```

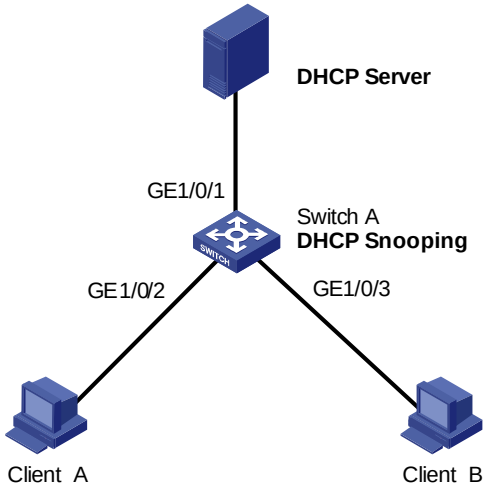
ARP Attack Detection Configuration Example

Network requirements

As shown in Figure 1-4, GigabitEthernet 1/0/1 of Switch A connects to DHCP Server; GigabitEthernet 1/0/2 connects to Client A, GigabitEthernet 1/0/3 connects to Client B. GigabitEthernet 1/0/1, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 belong to VLAN 1.

- Enable DHCP snooping on Switch A and specify GigabitEthernet 1/0/1 as the DHCP snooping trusted port.
- Enable ARP attack detection in VLAN 1 to prevent ARP man-in-the-middle attacks, and specify GigabitEthernet 1/0/1 as the ARP trusted port.

Figure 1-4 ARP attack detection configuration



Configuration procedure

Enable DHCP snooping on Switch A.

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

Specify GigabitEthernet 1/0/1 as the DHCP snooping trusted port and the ARP trusted port.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/1] arp detection trust
[SwitchA-GigabitEthernet1/0/1] quit
```

Enable ARP attack detection on all ports in VLAN 1.

```
[SwitchA] vlan 1
[SwitchA-vlan1] arp detection enable
```

Table of Contents

1 SNMP Configuration 1-1
SNMP Overview 1-1
SNMP Operation Mechanism 1-1
SNMP Versions 1-1
Supported MIBs 1-2
Configuring Basic SNMP Functions 1-3
Configuring Trap Parameters 1-5
Configuring Basic Trap 1-5
Configuring Extended Trap 1-6
Enabling Logging for Network Management 1-7
Displaying and Maintaining SNMP 1-7
SNMP Configuration Examples 1-7
SNMP Configuration Examples 1-7
2 RMON Configuration 2-1
Introduction to RMON 2-1
Working Mechanism of RMON 2-1
Commonly Used RMON Groups 2-2
RMON Configuration 2-3
Displaying and Maintaining RMON 2-4
RMON Configuration Examples 2-4

1 SNMP Configuration



Note

- The term switch used throughout this document refers to a switching device in a generic sense or the switching engine of a WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

SNMP Overview

The simple network management protocol (SNMP) is used for ensuring the transmission of the management information between any two network nodes. In this way, network administrators can easily retrieve and modify the information about any node on the network. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

As SNMP adopts the polling mechanism and provides basic function set, it is suitable for small-sized networks with fast-speed and low-cost. SNMP is based on user datagram protocol (UDP) and is thus widely supported by many products.

SNMP Operation Mechanism

SNMP is implemented by two components, namely, network management station (NMS) and agent.

- An NMS can be a workstation running client program. At present, the commonly used network management platforms include QuidView, Sun NetManager, IBM NetView, and so on.
- Agent is server-side software running on network devices.

An NMS can send GetRequest, GetNextRequest and SetRequest messages to the agents. Upon receiving the requests from the NMS, an agent performs Read or Write operation on the managed object (MIB, Management Information Base) according to the message types, generates the corresponding Response packets and returns them to the NMS.

When a network device operates improperly or changes to other state, the agent on it can also send trap messages on its own initiative to the NMS to report the events.

SNMP Versions

Currently, SNMP agent on the device supports SNMPv3, and is compatible with SNMPv1 and SNMPv2c.

SNMPv3 adopts user name and password authentication.

SNMPv1 and SNMPv2c adopt community name authentication. The SNMP packets containing invalid community names are discarded. SNMP community name is used to define the relationship between

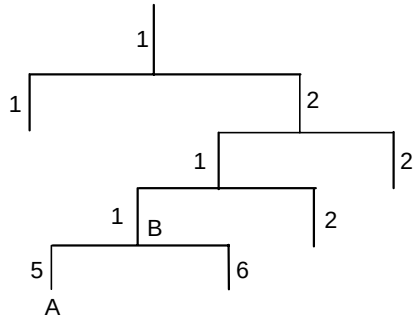
SNMP NMS and SNMP agent. Community name functions as password. It can limit accesses made by SNMP NMS to SNMP agent. You can perform the following community name-related configuration.

- Specifying MIB view that a community can access.
- Set the permission for a community to access an MIB object to be read-only or read-write. Communities with read-only permissions can only query the device information, while those with read-write permission can configure the device as well.
- Set the basic ACL specified by the community name.

Supported MIBs

An SNMP packet carries management variables with it. Management variable is used to describe the management objects of the device. To uniquely identify the management objects of the device, SNMP adopts a hierarchical naming scheme to organize the managed objects. It is like a tree, with each tree node representing a managed object, as shown in Figure 1-1. Each node in this tree can be uniquely identified by a path starting from the root.

Figure 1-1 Architecture of the MIB tree



The management information base (MIB) describes the hierarchical architecture of the tree and it is the set defined by the standard variables of the monitored network devices. In the above figure, the managed object B can be uniquely identified by a string of numbers {1.2.1.1}. The number string is the object identifier (OID) of the managed object.

The common MIBs supported by devices are listed in Table 1-1.

Table 1-1 Common MIBs

MIB attribute	MIB content	Related RFC
Public MIB	MIB II based on TCP/IP network device	RFC 1213
	BRIDGE MIB	RFC 1493
		RFC 2675
	RIP MIB	RFC 1724
	RMON MIB	RFC 2819
	Ethernet MIB	RFC 2665
	OSPF MIB	RFC 1253
	IF MIB	RFC 1573

MIB attribute	MIB content	Related RFC
Private MIB	DHCP MIB	—
	QACL MIB	
	MSTP MIB	
	VLAN MIB	
	IPV6 ADDRESS MIB	
	MIRRORGROUP MIB	
	QINQ MIB	
	802.x MIB	
	HGMP MIB	
	NTP MIB	
	Device management	
	Interface management	

Configuring Basic SNMP Functions

Because the configuration of SNMPv3 is quite different from that of SNMPv1 and SNMPv2c, their configuration procedures are described in two subsections.

Configuring basic SNMP functions for SNMPv1 or SNMPv2c

Follow these steps to configure basic SNMP functions for SNMPv1 or SNMPv2c:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable SNMP agent	**snmp-agent**	Optional Disabled by default. You can enable SNMP agent by executing this command or any of the commands used to configure SNMP agent.
Set system information, and specify to enable SNMPv1 or SNMPv2c on the device	**snmp-agent sys-info** { **contact** *sys-contact* | **location** *sys-location* | **version** { { **v1** | **v2c** | **v3** }* | **all** } }	Required By default, the contact information for system maintenance is "3Com Corporation.", the system location is "Marlborough, MA 01752 USA", and the SNMP version is None.

To do…			Use the command…	Remarks
Set a community name and access permission	Direct configuration	Set a community name	**snmp-agent community** { **read | write** } *community-name* [**acl** *acl-number* | **mib-view** *view-name*]*	Required • You can set an SNMPv1/SNMPv2c community name through direct configuration. • Indirect configuration is compatible with SNMPv3. The added user is equal to the community name for SNMPv1 and SNMPv2c. • You can choose either of them as needed.
	Indirect configuration	Set an SNMP group	**snmp-agent group** { **v1 | v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	
		Add a user to an SNMP group	**snmp-agent usm-user** { **v1 | v2c** } *user-name group-name* [**acl** *acl-number*]	
Set the maximum size of an SNMP packet for SNMP agent to receive or send			**snmp-agent packet max-size** *byte-count*	Optional 1,500 bytes by default.
Set the device engine ID			**snmp-agent local-engineid** *engineid*	Optional By default, the device engine ID is “enterprise number + device information”.
Create/Update the view information			**snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree* [**mask** *mask-value*]	Optional By default, the view name is “ViewDefault” and OID is 1.

Configuring basic SNMP functions for SNMPv3

The device now supports the Advanced Encryption Standard (AES) for SNMPv3 to provide encryption. AES can provide higher security than the Data Encryption Standard (DES).

Follow these steps to configure basic SNMP functions for SNMPv3:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable SNMP agent	**snmp-agent**	Optional Disabled by default. You can enable SNMP agent by executing this command or any of the commands used to configure SNMP agent.
Set system information and specify to enable SNMPv3 on the device	**snmp-agent sys-info** { **contact** *sys-contact* | **location** *sys-location* | **version** { { **v1** | **v2c** | **v3** }* | **all** } }	Required By default, the contact information for system maintenance is "3Com Corporation", the system location is "Marlborough, MA 01752 USA", and the SNMP version is None.

To do…	Use the command…	Remarks
Set an SNMP group	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	Required
Encrypt a plain-text password to generate a cipher-text one	**snmp-agent calculate-password** *plain-password* **mode** { **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }	Optional This command is used if password in cipher-text is needed for adding a new user.
Add a user to an SNMP group	**snmp-agent usm-user v3** *user-name group-name* [**cipher**] [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **des56** | **aes128** } *priv-password*]] [**acl** *acl-number*]	Required
Set the maximum size of an SNMP packet for SNMP agent to receive or send	**snmp-agent packet max-size** *byte-count*	Optional 1,500 bytes by default.
Set the device engine ID	**snmp-agent local-engineid** *engineid*	Optional By default, the device engine ID is “enterprise number + device information”.
Create or update the view information	**snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree* [**mask** *mask-value*]	Optional By default, the view name is “ViewDefault” and OID is 1.

Note

The device provides the following functions to prevent attacks through unused UDP ports.

- Executing the **snmp-agent** command or any of the commands used to configure SNMP agent enables the SNMP agent, and at the same opens UDP port 161 and UDP port 1024 used by SNMP agents and SNMP trap clients respectively.
- Executing the **undo snmp-agent** command disables the SNMP function and closes UDP port 161 and UDP port 1024 as well.

Configuring Trap Parameters

Configuring Basic Trap

Trap messages refer to those sent by managed devices to the NMS without request. They are used to report some urgent and important events (for example, the rebooting of managed devices).

Note that basic SNMP configuration is performed before you configure basic trap.

Follow these steps to configure basic Trap:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enable the device to send Trap messages to NMS		**snmp-agent trap enable** [**configuration** | **flash** | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system** |]	Optional By default, a port is enabled to send all types of Traps.
Enable the port to send Trap messages	Enter port view or interface view	**interface** *interface-type interface-number*	
	Enable the port or interface to send Trap messages	**enable snmp trap updown**	
	Quit to system view	**quit**	
Set the destination for Trap messages		**snmp-agent target-host trap address udp-domain** { *ip-address* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** {**authentication** | **privacy** }]	Required
Set the source address for Trap messages		**snmp-agent trap source** *interface-type interface-number*	Optional
Set the size of the queue used to hold the Traps to be sent to the destination host		**snmp-agent trap queue-size** *size*	Optional The default is 100.
Set the aging time for Trap messages		**snmp-agent trap life** *seconds*	Optional 120 seconds by default.

Configuring Extended Trap

The extended Trap includes the following.

- “Interface description” and “interface type” are added into the linkUp/linkDown Trap message. When receiving this extended Trap message, NMS can immediately determine which interface on the device fails according to the interface description and type.
- In all Trap messages sent from the information center to the log server, a MIB object name is added after the OID field of the MIB object. The name is for your better understanding of the MIB object.

Follow these steps to configure extended Trap:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure extended Trap	**snmp-agent trap ifmib link extended**	Optional By default, the linkUp/linkDown Trap message adopts the standard format defined in IF-MIB. For details, refer to RFC 1213.

Enabling Logging for Network Management

Follow these steps to enable logging for network management:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable logging for network management	**snmp-agent log** { **set-operation** | **get-operation** | **all** }	Optional Disabled by default.

Note

Use the **display logbuffer** command to view the log of the get and set operations requested by the NMS.

Displaying and Maintaining SNMP

To do…	Use the command…	Remarks
Display the SNMP information about the current device	**display snmp-agent sys-info** [**contact** | **location** | **version**]*	Available in any view
Display SNMP packet statistics	**display snmp-agent statistics**	
Display the engine ID of the current device	**display snmp-agent** { **local-engineid** | **remote-engineid** }	
Display group information about the device	**display snmp-agent group** [*group-name*]	
Display SNMP user information	**display snmp-agent usm-user** [**engineid** *engineid* | **username** *user-name* | **group** *group-name*]	
Display Trap list information	**display snmp-agent trap-list**	
Display the currently configured community name	**display snmp-agent community** [**read** | **write**]	
Display the currently configured MIB view	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]	

SNMP Configuration Examples

SNMP Configuration Examples

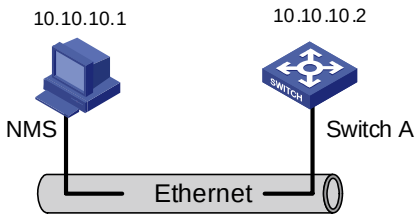
Network requirements

- As shown in Figure 1-2, an NMS and Switch A (SNMP agent) are connected through the Ethernet. The IP address of the NMS is 10.10.10.1 and that of the VLAN interface on Switch A is 10.10.10.2.

- Perform the following configuration on Switch A: setting the community name and access permission, administrator ID, contact and location of Switch A, and enabling the device to sent trap messages.

Thus, the NMS is able to access Switch A and receive the trap messages sent by Switch A.

Figure 1-2 Network diagram for SNMP configuration



Network procedure

Enable SNMP agent, and set the SNMPv1 and SNMPv2c community names.

```
<device> system-view
[device] snmp-agent
[device] snmp-agent sys-info version all
[device] snmp-agent community read public
[device] snmp-agent community write private
```

Set the access right of the NMS to the MIB of the SNMP agent.

```
[device] snmp-agent mib-view include internet 1.3.6.1
```

For SNMPv3, set:

- SNMPv3 group and user
- security to the level of needing authentication and encryption
- authentication protocol to HMAC-MD5
- authentication password to passmd5
- encryption protocol to AES
- encryption password to cfb128cfb128

```
[device] snmp-agent group v3 managev3group privacy write-view internet
[device] snmp-agent usm-user v3 managev3user managev3group authentication-mode md5 passmd5
privacy-mode aes128 cfb128cfb128
```

Set the VLAN-interface 2 as the interface used by NMS. Add port GigabitEthernet 1/0/2, which is to be used for network management, to VLAN 2. Set the IP address of VLAN-interface 2 as 10.10.10.2.

```
[device] vlan 2
[device-vlan2] port Ethernet 1/0/2
[device-vlan2] quit
[device] interface Vlan-interface 2
[device-Vlan-interface2] ip address 10.10.10.2 255.255.255.0
[device-Vlan-interface2] quit
```

Enable the SNMP agent to send Trap messages to the NMS whose IP address is 10.10.10.1. The SNMP community name to be used is “public”.

```
[device] snmp-agent trap enable standard authentication
[device] snmp-agent trap enable standard coldstart
[device] snmp-agent trap enable standard linkup
```

```
[device] snmp-agent trap enable standard linkdown
[device] snmp-agent target-host trap address udp-domain 10.10.10.1 udp-port 5000 params
securityname public
```

Configuring the NMS

The device supports iMC NMS. SNMPv3 adopts user name and password authentication. When you use the iMC, you need to set user names and choose the security level in. For each security level, you need to set authorization mode, authorization password, encryption mode, encryption password, and so on. In addition, you need to set timeout time and maximum retry times.

You can query and configure the device through the NMS. For more information, refer to the corresponding manuals of network management products.



Note

Authentication-related configuration on the NMS must be consistent with that of the devices for the NMS to manage the devices successfully.

---

2 RMON Configuration

Introduction to RMON

Remote monitoring (RMON) is a kind of management information base (MIB) defined by Internet Engineering Task Force (IETF). It is an important enhancement made to MIB II standards. RMON is mainly used to monitor the data traffic across a network segment or even the entire network, and is currently a commonly used network management standard.

An RMON system comprises of two parts: the network management station (NMS) and the agents running on network devices. RMON agents operate on network monitors or network probes to collect and keep track of the statistics of the traffic across the network segments to which their ports connect, such as the total number of the packets on a network segment in a specific period of time and the total number of packets successfully sent to a specific host.

- RMON is fully based on SNMP architecture. It is compatible with the current SNMP implementations.
- RMON enables SNMP to monitor remote network devices more effectively and actively, thus providing a satisfactory means of monitoring remote subnets.
- With RMON implemented, the communication traffic between NMS and SNMP agents can be reduced, thus facilitating the management of large-scale internetworks.

Working Mechanism of RMON

RMON allows multiple monitors. It can collect data in the following two ways:

- Using the dedicated RMON probes. When an RMON system operates in this way, the NMS directly obtains management information from the RMON probes and controls the network resources. In this case, all information in the RMON MIB can be obtained.
- Embedding RMON agents into network devices (such as routers, switches and hubs) directly to make the latter capable of RMON probe functions. When an RMON system operates in this way, the NMS collects network management information by exchanging information with the SNMP agents using the basic SNMP commands. However, this way depends on device resources heavily and an NMS operating in this way can only obtain the information about these four groups (instead of all the information in the RMON MIB): alarm group, event group, history group, and statistics group.

The device implements RMON in the second way. With an RMON agent embedded in, the device can serve as a network device with the RMON probe function. Through the RMON-capable SNMP agents running on the device, an NMS can obtain the information about the total traffic, error statistics and performance statistics of the network segments to which the ports of the managed network devices are connected. Thus, the NMS can further manage the networks.

Commonly Used RMON Groups

Event group

Event group is used to define the indexes of events and the processing methods of the events. The events defined in an event group are mainly used by entries in the alarm group and extended alarm group to trigger alarms.

You can specify a network device to act in one of the following ways in response to an event:

- Logging the event
- Sending trap messages to the NMS
- Logging the event and sending trap messages to the NMS
- No processing

Alarm group

RMON alarm management enables monitoring on specific alarm variables (such as the statistics of a port). When the value of a monitored variable exceeds the threshold, an alarm event is generated, which then triggers the network device to act in the way defined in the events. Events are defined in event groups.

With an alarm entry defined in an alarm group, a network device performs the following operations accordingly:

- Sampling the defined alarm variables periodically
- Comparing the samples with the threshold and triggering the corresponding events if the former exceed the latter

Extended alarm group

With extended alarm entry, you can perform operations on the samples of alarm variables and then compare the operation results with the thresholds, thus implement more flexible alarm functions.

With an extended alarm entry defined in an extended alarm group, the network devices perform the following operations accordingly:

- Sampling the alarm variables referenced in the defined extended alarm expressions periodically
- Performing operations on the samples according to the defined expressions
- Comparing the operation results with the thresholds and triggering corresponding events if the operation result exceeds the thresholds.

History group

After a history group is configured, the device collects network statistics information periodically and stores the statistics information temporarily for later use. A history group can provide the history data of the statistics on network segment traffic, error packets, broadcast packets, and bandwidth utilization.

With the history data management function, you can configure network devices to collect history data, sample and store data of a specific port periodically.

Statistics group

Statistics group contains the statistics of each monitored port on the device. An entry in a statistics group is an accumulated value counting from the time when the statistics group is created.

The statistics include the number of the following items: collisions, packets with cyclic redundancy check (CRC) errors, undersize (or oversize) packets, broadcast packets, multicast packets, and received bytes and packets.

With the RMON statistics management function, you can monitor the use of a port and make statistics on the errors occurred when the ports are being used.

RMON Configuration

Before performing RMON configuration, make sure the SNMP agents are correctly configured. For the information about SNMP agent configuration, refer to Configuring Basic SNMP Functions.

Follow these steps to configure RMON:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Add an event entry	**rmon event** *event-entry* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *text*]	Optional
Add an alarm entry	**rmon alarm** *entry-number alarm-variable sampling-time* { **delta** | **absolute** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* [**owner** *text*]	Optional Before adding an alarm entry, you need to use the **rmon event** command to define the event to be referenced by the alarm entry.
Add an extended alarm entry	**rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-timer* { **delta** | **absolute** | **changeratio** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]	Optional Before adding an extended alarm entry, you need to use the **rmon event** command to define the event to be referenced by the extended alarm entry.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add a history entry	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]	Optional
Add a statistics entry	**rmon statistics** *entry-number* [**owner** *text*]	Optional

Note

- The **rmon alarm** and **rmon prialarm** commands take effect on existing nodes only.
- For each port, only one RMON statistics entry can be created. That is, if an RMON statistics entry is already created for a given port, you will fail to create another statistics entry with a different index for the same port.

Displaying and Maintaining RMON

To do…	Use the command…	Remarks
Display RMON statistics	**display rmon statistics** [*interface-type interface-number* | **unit** *unit-number*]	Available in any view
Display RMON history information	**display rmon history** [*interface-type interface-number* | **unit** *unit-number*]	
Display RMON alarm information	**display rmon alarm** [*entry-number*]	
Display extended RMON alarm information	**display rmon prialarm** [*prialarm-entry-number*]	
Display RMON events	**display rmon event** [*event-entry*]	
Display RMON event logs	**display rmon eventlog** [*event-entry*]	

RMON Configuration Examples

Network requirements

- As shown in Figure 2-1, the Switch to be tested is connected to a remote NMS through the Internet. Ensure that the SNMP agents are correctly configured before performing RMON configuration.
- Create an entry in the extended alarm table to monitor the information of statistics on the Ethernet port, if the change rate of which exceeds the set threshold, the alarm events will be triggered.

Figure 2-1 Network diagram for RMON configuration



Configuration procedures

Add the statistics entry numbered 1 to take statistics on GigabitEthernet 1/0/1.

```
<device> system-view
[device] interface GigabitEthernet 1/0/1
[device-GigabitEthernet1/0/1] rmon statistics 1
[device-GigabitEthernet1/0/1] quit
```

Add the event entries numbered 1 and 2 to the event table, which will be triggered by the following extended alarm.

```
[device] rmon event 1 log
[device] rmon event 2 trap 10.21.30.55
```

Add an entry numbered 2 to the extended alarm table to allow the system to calculate the alarm variables with the (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1) formula to get the numbers of all the oversize and undersize packets received by GigabitEthernet 1/0/1 that are in correct data format and sample it in every 10 seconds. When the change ratio between samples reaches the rising threshold of 50, event 1 is triggered; when the change ratio drops under the falling threshold, event 2 is triggered.

```
[device] rmon prialarm 2 (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1) test 10
changeratio rising_threshold 50 1 falling_threshold 5 2 entrytype forever owner user1
```

Display the RMON extended alarm entry numbered 2.

```
[device] display rmon prialarm 2
Prialarm table 2 owned by user1 is VALID.
  Samples type            : changeratio
  Variable formula : (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1)
  Description             : test
  Sampling interval      : 10(sec)
  Rising threshold       : 100(linked with event 1)
  Falling threshold      : 10(linked with event 2)
  When startup enables  : risingOrFallingAlarm
  This entry will exist : forever.
  Latest value            : 0
```

Table of Contents

1 Multicast Overview 1-1
Multicast Overview 1-1
Information Transmission in the Unicast Mode 1-1
Information Transmission in the Broadcast Mode 1-2
Information Transmission in the Multicast Mode 1-3
Roles in Multicast 1-4
Advantages and Applications of Multicast 1-5
Multicast Models 1-5
Multicast Architecture 1-6
Multicast Protocols 1-9
Multicast Packet Forwarding Mechanism 1-11
Implementation of the RPF Mechanism 1-11
RPF Check 1-12

2 IGMP Snooping Configuration 2-1
IGMP Snooping Overview 2-1
Principle of IGMP Snooping 2-1
Basic Concepts in IGMP Snooping 2-1
Work Mechanism of IGMP Snooping 2-2
IGMP Snooping Configuration 2-4
IGMP Snooping Configuration Task List 2-4
Enabling IGMP Snooping 2-5
Configuring the Version of IGMP Snooping 2-5
Configuring Timers 2-6
Configuring Fast Leave Processing 2-6
Configuring a Multicast Group Filter 2-7
Configuring the Maximum Number of Multicast Groups on a Port 2-8
Configuring IGMP Querier 2-9
Suppressing Flooding of Unknown Multicast Traffic in a VLAN 2-10
Configuring Static Member Port for a Multicast Group 2-10
Configuring a Static Router Port 2-11
Configuring a Port as a Simulated Group Member 2-12
Configuring a VLAN Tag for Query Messages 2-13
Configuring Multicast VLAN 2-13
Displaying and Maintaining IGMP Snooping 2-15
IGMP Snooping Configuration Examples 2-15
Configuring IGMP Snooping 2-15
Configuring Multicast VLAN 2-17
Troubleshooting IGMP Snooping 2-19

3 Common Multicast Configuration 3-1
Common Multicast Configuration 3-1
Configuring a Multicast MAC Address Entry 3-1
Configuring Dropping Unknown Multicast Packets 3-2
Displaying and Maintaining Common Multicast Configuration 3-2

1 Multicast Overview

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of the WX3000 series devices.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Multicast Overview

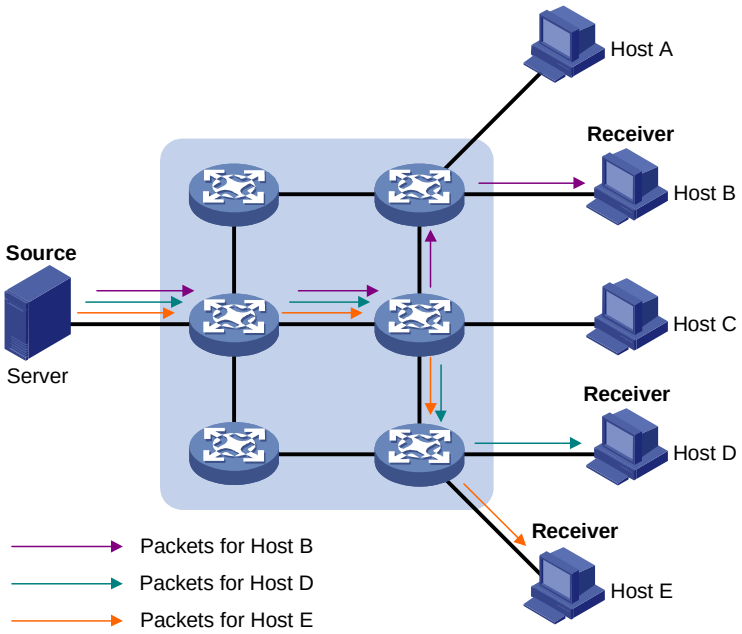
With development of networks on the Internet, more and more interaction services such as data, voice, and video services are running on the networks. In addition, highly bandwidth- and time-critical services, such as e-commerce, Web conference, online auction, video on demand (VoD), and tele-education have come into being. These services have higher requirements for information security, legal use of paid services, and network bandwidth.

In the network, packets are sent in three modes: unicast, broadcast and multicast. The following sections describe and compare data interaction processes in unicast, broadcast, and multicast.

Information Transmission in the Unicast Mode

In unicast, the system establishes a separate data transmission channel for each user requiring this information, and sends a separate copy of the information to the user, as shown in Figure 1-1:

Figure 1-1 Information transmission in the unicast mode

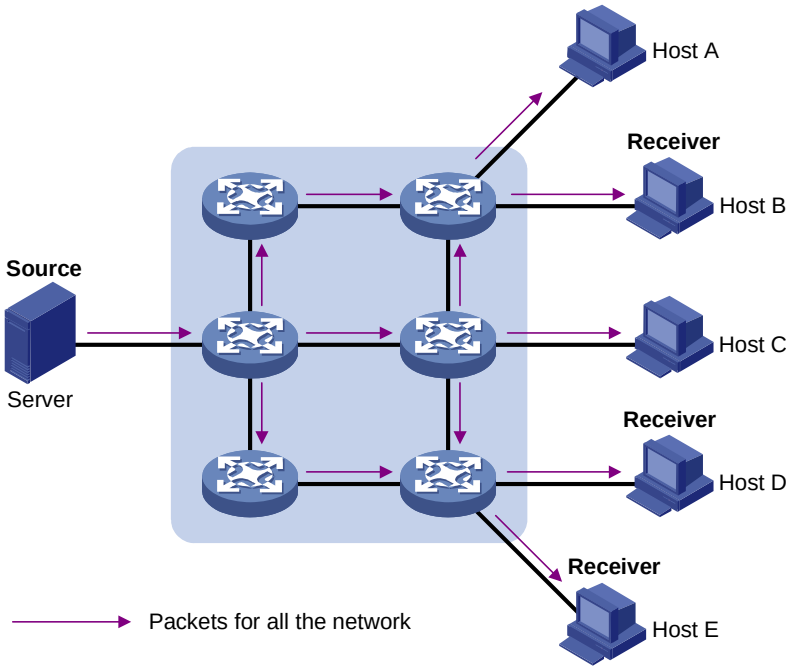


Assume that Hosts B, D and E need this information. The source server establishes transmission channels for the devices of these users respectively. As the transmitted traffic over the network is in direct proportion to the number of users that receive this information, when a large number of users need this information, the server must send many pieces of information with the same content to the users. Therefore, the limited bandwidth becomes the bottleneck in information transmission. This shows that unicast is not good for the transmission of a great deal of information.

Information Transmission in the Broadcast Mode

When you adopt broadcast, the system transmits information to all users on a network. Any user on the network can receive the information, no matter the information is needed or not. Figure 1-2shows information transmission in broadcast mode.

Figure 1-2 Information transmission in the broadcast mode



Assume that Hosts B, D, and E need the information. The source server broadcasts this information through routers, and Hosts A and C on the network also receive this information.

As we can see from the information transmission process, the security and legal use of paid service cannot be guaranteed. In addition, when only a small number of users on the same network need the information, the utilization ratio of the network resources is very low and the bandwidth resources are greatly wasted.

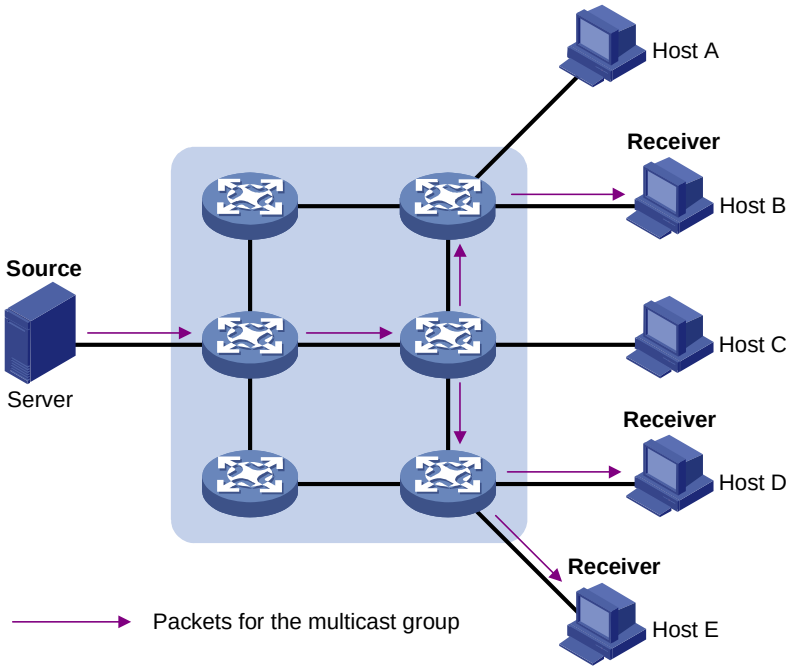
Therefore, broadcast is disadvantageous in transmitting data to specific users; moreover, broadcast occupies large bandwidth.

Information Transmission in the Multicast Mode

As described in the previous sections, unicast is suitable for networks with sparsely distributed users, whereas broadcast is suitable for networks with densely distributed users. When the number of users requiring information is not certain, unicast and broadcast deliver a low efficiency.

Multicast solves this problem. When some users on a network require specified information, the multicast information sender (namely, the multicast source) sends the information only once. With multicast distribution trees established for multicast data packets through multicast routing protocols, the packets are duplicated and distributed at the nearest nodes, as shown in Figure 1-3:

Figure 1-3 Information transmission in the multicast mode



Assume that Hosts B, D and E need the information. To transmit the information to the right users, it is necessary to group Hosts B, D and E into a receiver set. The routers on the network duplicate and distribute the information based on the distribution of the receivers in this set. Finally, the information is correctly delivered to Hosts B, D, and E.

The advantages of multicast over unicast are as follows:

- No matter how many receivers exist, there is only one copy of the same multicast data flow on each link.
- With the multicast mode used to transmit information, an increase of the number of users does not add to the network burden remarkably.

The advantages of multicast over broadcast are as follows:

- A multicast data flow can be sent only to the receiver that requires the data.
- Multicast brings no waste of network resources and makes proper use of bandwidth.

Roles in Multicast

The following roles are involved in multicast transmission:

- An information sender is referred to as a multicast source (“Source” in Figure 1-3).
- Each receiver is a multicast group member (“Receiver” in Figure 1-3).
- All receivers interested in the same information form a multicast group. Multicast groups are not subject to geographic restrictions.
- A router that supports Layer 3 multicast is called multicast router or Layer 3 multicast device. In addition to providing multicast routing, a multicast router can also manage multicast group members.

For a better understanding of the multicast concept, you can assimilate multicast transmission to the transmission of TV programs, as shown in Table 1-1.

Table 1-1 An analogy between TV transmission and multicast transmission

Step	TV transmission	Multicast transmission
1	A TV station transmits a TV program through a television channel.	A multicast source sends multicast data to a multicast group.
2	A user tunes the TV set to the channel.	A receiver joins the multicast group.
3	The user starts to watch the TV program transmitted by the TV station via the channel.	The receiver starts to receive the multicast data that the source sends to the multicast group.
4	The user turns off the TV set.	The receiver leaves the multicast group.

Note

- A multicast source does not necessarily belong to a multicast group. Namely, a multicast source is not necessarily a multicast data receiver.
- A multicast source can send data to multiple multicast groups at the same time, and multiple multicast sources can send data to the same multicast group at the same time.

Advantages and Applications of Multicast

Advantages of multicast

Advantages of multicast include:

- Enhanced efficiency: Multicast decreases network traffic and reduces server load and CPU load.
- Optimal performance: Multicast reduces redundant traffic.
- Distributive application: Multicast makes multiple-point application possible.

Application of multicast

The multicast technology effectively addresses the issue of point-to-multipoint data transmission. By enabling high-efficiency point-to-multipoint data transmission, over an IP network, multicast greatly saves network bandwidth and reduces network load.

Multicast provides the following applications:

- Applications of multimedia and flow media, such as Web TV, Web radio, and real-time video/audio conferencing.
- Communication for training and cooperative operations, such as remote education.
- Database and financial applications (stock), and so on.
- Any point-to-multiple-point data application.

Multicast Models

Based on the multicast source processing modes, there are three multicast models:

- Any-Source Multicast (ASM)
- Source-Filtered Multicast (SFM)
- Source-Specific Multicast (SSM)

ASM model

In the ASM model, any sender can become a multicast source and send information to a multicast group; numbers of receivers can join a multicast group identified by a group address and obtain multicast information addressed to that multicast group. In this model, receivers are not aware of the position of a multicast source in advance. However, they can join or leave the multicast group at any time.

SFM model

The SFM model is derived from the ASM model. From the view of a sender, the two models have the same multicast group membership architecture.

Functionally, the SFM model is an extension of the ASM model. In the SFM model, the upper layer software checks the source address of received multicast packets so as to permit or deny multicast traffic from specific sources. Therefore, receivers can receive the multicast data from only part of the multicast sources. From the view of a receiver, multicast sources are not all valid: they are filtered.

SSM model

In the practical life, users may be interested in the multicast data from only certain multicast sources. The SSM model provides a transmission service that allows users to specify the multicast sources they are interested in at the client side.

The radical difference between the SSM model and the ASM model is that in the SSM model, receivers already know the locations of the multicast sources by some means. In addition, the SSM model uses a multicast address range that is different from that of the ASM model, and dedicated multicast forwarding paths are established between receivers and the specified multicast sources.

Multicast Architecture

The purpose of IP multicast is to transmit information from a multicast source to receivers in the multicast mode and to satisfy information requirements of receivers. You should be concerned about:

- Host registration: What receivers reside on the network?
- Technologies of discovering a multicast source: Which multicast source should the receivers receive information from?
- Multicast addressing mechanism: Where should the multicast source transports information?
- Multicast routing: How is information transported?

IP multicast is a kind of peer-to-peer service. Based on the protocol layer sequence from bottom to top, the multicast mechanism contains addressing mechanism, host registration, multicast routing, and multicast application:

- Addressing mechanism: Information is sent from a multicast source to a group of receivers through multicast addresses.
- Host registration: A receiving host joins and leaves a multicast group dynamically using the membership registration mechanism.
- Multicast routing: A router or switch transports packets from a multicast source to receivers by building a multicast distribution tree with multicast routes.
- Multicast application: A multicast source must support multicast applications, such as video conferencing. The TCP/IP protocol suite must support the function of sending and receiving multicast information.

Multicast Address

As receivers are multiple hosts in a multicast group, you should be concerned about the following questions:

- What destination should the information source send the information to in the multicast mode?
- How to select the destination address?

These questions are about multicast addressing. To enable the communication between the information source and members of a multicast group (a group of information receivers), network-layer multicast addresses, namely, IP multicast addresses must be provided. In addition, a technology must be available to map IP multicast addresses to link-layer MAC multicast addresses. The following sections describe these two types of multicast addresses:

IP multicast address

Internet Assigned Numbers Authority (IANA) categorizes IP addresses into five classes: A, B, C, D, and E. Unicast packets use IP addresses of Class A, B, and C based on network scales. Class D IP addresses are used as destination addresses of multicast packets. Class D address must not appear in the IP address field of a source IP address of IP packets. Class E IP addresses are reserved for future use.

In unicast data transport, a data packet is transported hop by hop from the source address to the destination address. In an IP multicast environment, there are a group of destination addresses (called group address), rather than one address. All the receivers join a group. Once they join the group, the data sent to this group of addresses starts to be transported to the receivers. All the members in this group can receive the data packets. This group is a multicast group.

A multicast group has the following characteristics:

- The membership of a group is dynamic. A host can join and leave a multicast group at any time.
- A multicast group can be either permanent or temporary.
- A multicast group whose addresses are assigned by IANA is a permanent multicast group. It is also called reserved multicast group.

Note that:

- The IP addresses of a permanent multicast group keep unchanged, while the members of the group can be changed.
- There can be any number of, or even zero, members in a permanent multicast group.
- Those IP multicast addresses not assigned to permanent multicast groups can be used by temporary multicast groups.

Class D IP addresses range from 224.0.0.0 to 239.255.255.255. For details, see Table 1-2.

Table 1-2 Range and description of Class D IP addresses

Class D address range	Description
224.0.0.0 to 224.0.0.255	Reserved multicast addresses (IP addresses for permanent multicast groups). The IP address 224.0.0.0 is reserved. Other IP addresses can be used by routing protocols.
224.0.1.0 to 231.255.255.255 233.0.0.0 to 238.255.255.255	Available any-source multicast (ASM) multicast addresses (IP addresses for temporary groups). They are valid for the entire network.
232.0.0.0 to 232.255.255.255	Available source-specific multicast (SSM) multicast group addresses.

Class D address range	Description
239.0.0.0 to 239.255.255.255	Administratively scoped multicast addresses, which are for specific local use only.

As specified by IANA, the IP addresses ranging from 224.0.0.0 to 224.0.0.255 are reserved for network protocols on local networks. The following table lists commonly used reserved IP multicast addresses:

Table 1-3 Reserved IP multicast addresses

Class D address range	Description
224.0.0.1	Address of all hosts
224.0.0.2	Address of all multicast routers
224.0.0.3	Unassigned
224.0.0.4	Distance vector multicast routing protocol (DVMRP) routers
224.0.0.5	Open shortest path first (OSPF) routers
224.0.0.6	Open shortest path first designated routers (OSPF DR)
224.0.0.7	Shared tree routers
224.0.0.8	Shared tree hosts
224.0.0.9	RIP-2 routers
224.0.0.11	Mobile agents
224.0.0.12	DHCP server/relay agent
224.0.0.13	All protocol independent multicast (PIM) routers
224.0.0.14	Resource reservation protocol (RSVP) encapsulation
224.0.0.15	All core-based tree (CBT) routers
224.0.0.16	The specified subnetwork bandwidth management (SBM)
224.0.0.17	All SBMS
224.0.0.18	Virtual router redundancy protocol (VRRP)
224.0.0.19 to 224.0.0.255	Other protocols

Note

Like having reserved the private network segment 10.0.0.0/8 for unicast, IANA has also reserved the network segment 239.0.0.0/8 for multicast. These are administratively scoped addresses. With the administratively scoped addresses, you can define the range of multicast domains flexibly to isolate IP addresses between different multicast domains, so that the same multicast address can be used in different multicast domains without causing collisions.

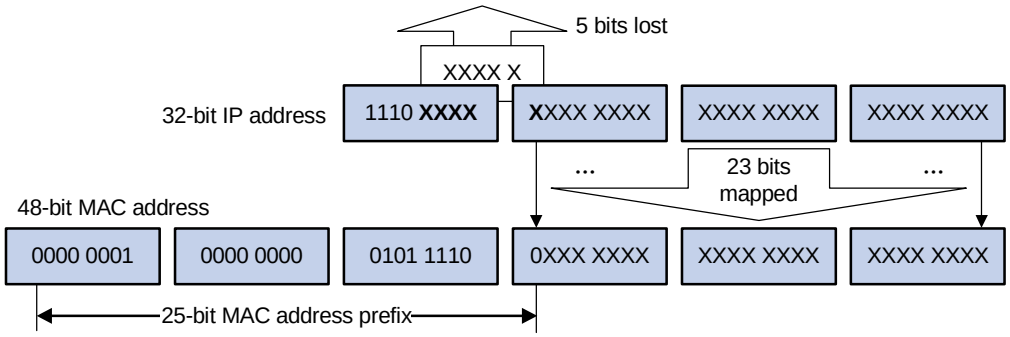
Ethernet multicast MAC address

When a unicast IP packet is transported in an Ethernet network, the destination MAC address is the MAC address of the receiver. When a multicast packet is transported in an Ethernet network, a

multicast MAC address is used as the destination address because the destination is a group with an uncertain number of members.

As stipulated by IANA, the high-order 24 bits of a multicast MAC address are 0x01005e, while the low-order 23 bits of a MAC address are the low-order 23 bits of the multicast IP address. Figure 1-4 describes the mapping relationship:

Figure 1-4 Multicast address mapping



The high-order four bits of the IP multicast address are 1110, representing the multicast ID. Only 23 bits of the remaining 28 bits are mapped to a MAC address. Thus, five bits of the multicast IP address are lost. As a result, 32 IP multicast addresses are mapped to the same MAC address.

Multicast Protocols

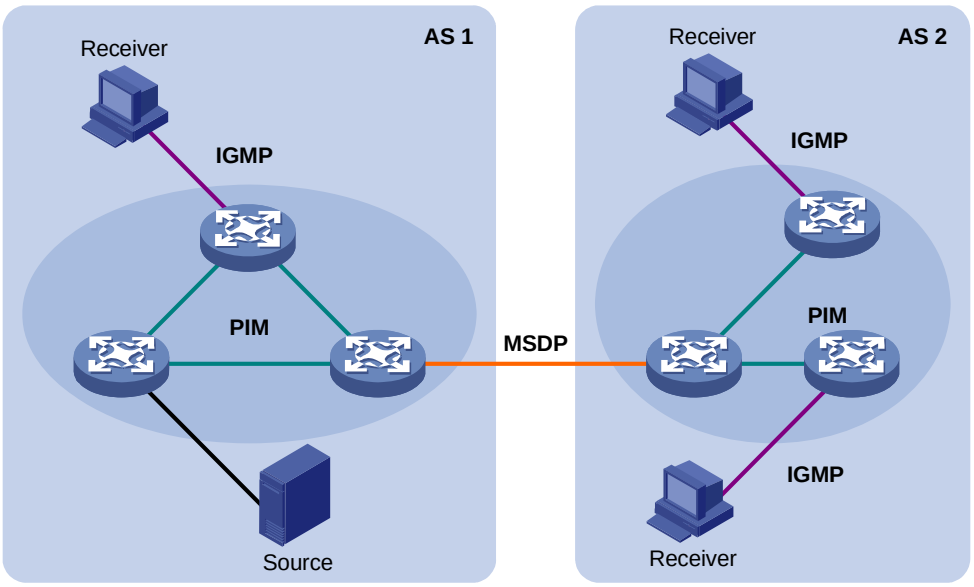
Note

- Generally, we refer to IP multicast working at the network layer as Layer 3 multicast and the corresponding multicast protocols as Layer 3 multicast protocols, which include IGMP, PIM, and MSDP; we refer to IP multicast working at the data link layer as Layer 2 multicast and the corresponding multicast protocols as Layer 2 multicast protocols, which include IGMP Snooping.
- This section provides only general descriptions about applications and functions of the Layer 2 and Layer 3 multicast protocols in a network. For details about these protocols, refer to the related chapters of this manual.

Layer 3 multicast protocols

Layer 3 multicast protocols include multicast group management protocols and multicast routing protocols. Figure 1-5 describes where these multicast protocols are in a network.

Figure 1-5 Positions of Layer 3 multicast protocols



1) Multicast management protocols

Typically, the Internet Group Management Protocol (IGMP) is used between hosts and Layer 3 multicast devices directly connected with the hosts. These protocols define the mechanism of establishing and maintaining group memberships between hosts and Layer 3 multicast devices.

2) Multicast routing protocols

A multicast routing protocol runs on Layer 3 multicast devices to establish and maintain multicast routes and forward multicast packets correctly and efficiently. Multicast routes constitute a loop-free data transmission path from a data source to multiple receivers, namely a multicast distribution tree.

In the ASM model, multicast routes come in intra-domain routes and inter-domain routes.

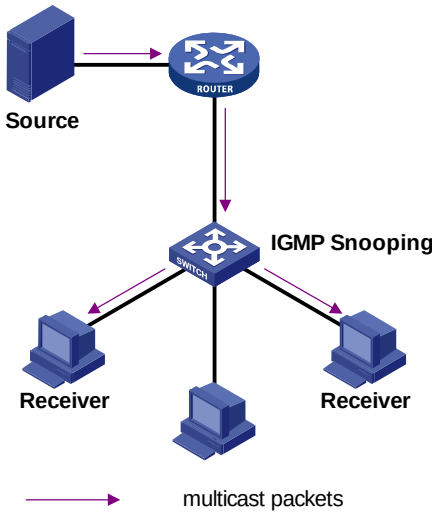
- An intra-domain multicast routing protocol is used to discover multicast sources and build multicast distribution trees within an autonomous system (AS) so as to deliver multicast data to receivers. Among a variety of mature intra-domain multicast routing protocols, protocol independent multicast (PIM) is a popular one. Based on the forwarding mechanism, PIM comes in two modes – dense mode (often referred to as PIM-DM) and sparse mode (often referred to as PIM-SM).
- An inter-domain multicast routing protocol is used for delivery of multicast information between two ASs. So far, mature solutions include multicast source discovery protocol (MSDP).

For the SSM model, multicast routes are not divided into inter-domain routes and intra-domain routes. Since receivers know the position of the multicast source, channels established through PIM-SM are sufficient for multicast information transport.

Layer 2 multicast protocols

Layer 2 multicast protocols include IGMP Snooping and multicast VLAN. Figure 1-6 shows where these protocols are in the network.

Figure 1-6 Positions of Layer 2 multicast protocols



2) IGMP Snooping

Running on Layer 2 devices, Internet Group Management Protocol Snooping (IGMP Snooping) are multicast constraining mechanisms that manage and control multicast groups by listening to and analyzing IGMP messages exchanged between the hosts and Layer 3 multicast devices, thus effectively controlling the flooding of multicast data in a Layer 2 network.

Multicast Packet Forwarding Mechanism

In a multicast model, a multicast source sends information to the host group identified by the multicast group address in the destination address field of the IP packets. Therefore, to deliver multicast packets to receivers located in different parts of the network, multicast routers on the forwarding path usually need to forward multicast packets received on one incoming interface to multiple outgoing interfaces. Compared with a unicast model, a multicast model is more complex in the following aspects.

- In the network, multicast packet transmission is based on the guidance of the multicast forwarding table derived from the unicast routing table or the multicast routing table specially provided for multicast.
- To process the same multicast information from different peers received on different interfaces of the same device, every multicast packet is subject to a reverse path forwarding (RPF) check on the incoming interface. The result of the RPF check determines whether the packet will be forwarded or discarded. The RPF check mechanism is the basis for most multicast routing protocols to implement multicast forwarding.

The RPF mechanism enables multicast devices to forward multicast packets correctly based on the multicast route configuration. In addition, the RPF mechanism also helps avoid data loops caused by various reasons.

Implementation of the RPF Mechanism

Upon receiving a multicast packet that a multicast source S sends to a multicast group G, the multicast device first searches its multicast forwarding table:

1) If the corresponding (S, G) entry exists, and the interface on which the packet actually arrived is the incoming interface in the multicast forwarding table, the router forwards the packet to all the outgoing interfaces.

2) If the corresponding (S, G) entry exists, but the interface on which the packet actually arrived is not the incoming interface in the multicast forwarding table, the multicast packet is subject to an RPF check.

- If the result of the RPF check shows that the RPF interface is the incoming interface of the existing (S, G) entry, this means that the (S, G) entry is correct but the packet arrived from a wrong path and is to be discarded.
- If the result of the RPF check shows that the RPF interface is not the incoming interface of the existing (S, G) entry, this means that the (S, G) entry is no longer valid. The router replaces the incoming interface of the (S, G) entry with the interface on which the packet actually arrived and forwards the packet to all the outgoing interfaces.

3) If no corresponding (S, G) entry exists in the multicast forwarding table, the packet is also subject to an RPF check. The router creates an (S, G) entry based on the relevant routing information and using the RPF interface as the incoming interface, and installs the entry into the multicast forwarding table.

- If the interface on which the packet actually arrived is the RPF interface, the RPF check is successful and the router forwards the packet to all the outgoing interfaces.
- If the interface on which the packet actually arrived is not the RPF interface, the RPF check fails and the router discards the packet.

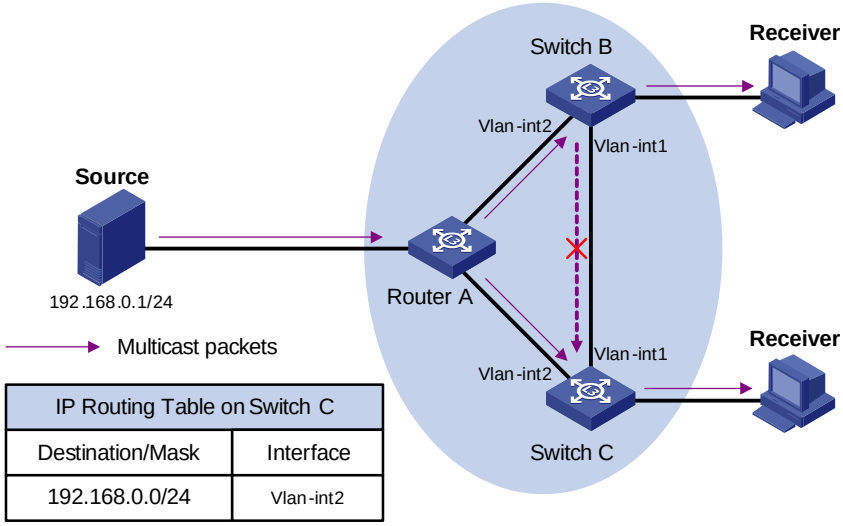
RPF Check

The basis for an RPF check is a unicast route. A unicast routing table contains the shortest path to each destination subnet. A multicast routing protocol does not independently maintain any type of unicast route; instead, it relies on the existing unicast routing information in creating multicast routing entries.

When performing an RPF check, a router searches its unicast routing table. The specific process is as follows: The router automatically chooses an optimal unicast route by searching its unicast routing table, using the IP address of the “packet source” as the destination address. The outgoing interface in the corresponding routing entry is the RPF interface and the next hop is the RPF neighbor. The router considers the path along which the packet from the RPF neighbor arrived on the RPF interface to be the shortest path that leads back to the source.

Assume that unicast routes exist in the network, as shown in Figure 1-7. Multicast packets travel along the SPT from the multicast source to the receivers.

Figure 1-7 RPF check process



- A multicast packet from Source arrives to VLAN-interface 1 of Switch C, and the corresponding forwarding entry does not exist in the multicast forwarding table of Switch C. Switch C performs an RPF check, and finds in its unicast routing table that the outgoing interface to 192.168.0.0/24 is VLAN-interface 2. This means that the interface on which the packet actually arrived is not the RPF interface. The RPF check fails and the packet is discarded.
- A multicast packet from Source arrives to VLAN-interface 2 of Switch C, and the corresponding forwarding entry does not exist in the multicast forwarding table of Switch C. The router performs an RPF check, and finds in its unicast routing table that the outgoing interface to 192.168.0.0/24 is the interface on which the packet actually arrived. The RPF check succeeds and the packet is forwarded.

2 IGMP Snooping Configuration

IGMP Snooping Overview

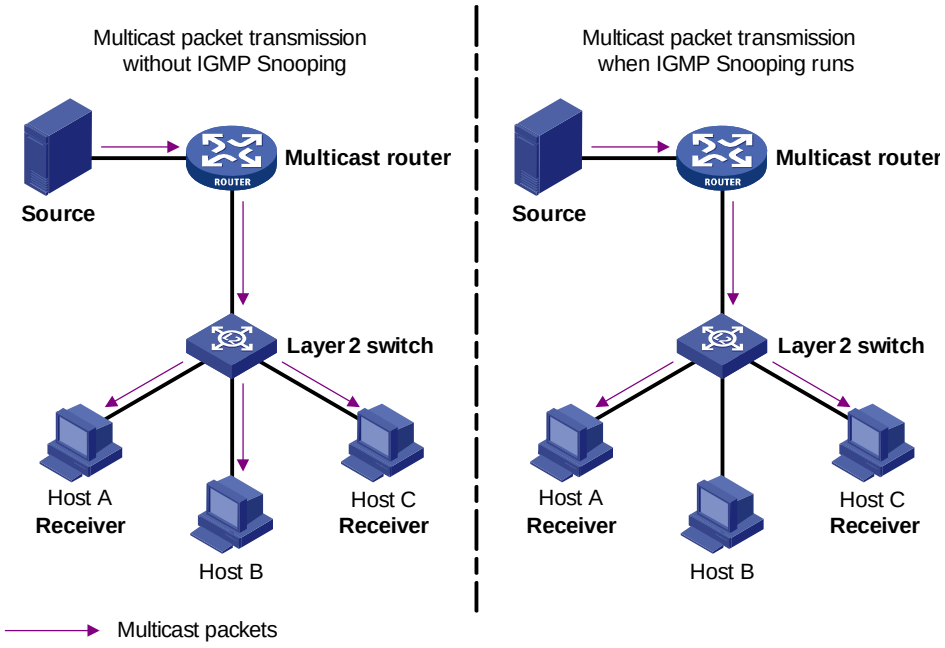
Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

Principle of IGMP Snooping

By analyzing received IGMP messages, a Layer 2 device running IGMP Snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings.

As shown in Figure 2-1, when IGMP Snooping is not running on the switch, multicast packets are broadcast to all devices at Layer 2. When IGMP Snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2.

Figure 2-1 Before and after IGMP Snooping is enabled on Layer 2 device

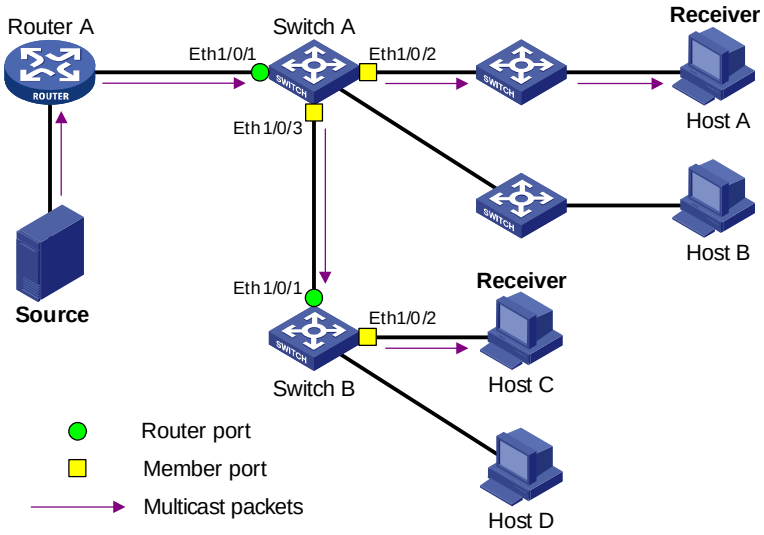


Basic Concepts in IGMP Snooping

IGMP Snooping related ports

As shown in Figure 2-2, Router A connects to the multicast source, IGMP Snooping runs on Switch A and Switch B, Host A and Host C are receiver hosts (namely, multicast group members).

Figure 2-2 IGMP Snooping related ports



Ports involved in IGMP Snooping, as shown in Figure 2-2, are described as follows:

- Router port: A router port is a port on the Layer 3 multicast device (DR or IGMP querier) side of the device. In the figure, Ethernet 1/0/1 of Switch A and Ethernet 1/0/1 of Switch B are router ports. A device registers all its local router ports in its router port list.
- Member port: A member port is a port on the multicast group member side of the device. In the figure, Ethernet 1/0/2 and Ethernet 1/0/3 of Switch A and Ethernet 1/0/2 of Switch B are member ports. A device records all member ports on the local device in the IGMP Snooping forwarding table.

Port aging timers in IGMP Snooping and related messages and actions

Table 2-1 Port aging timers in IGMP Snooping and related messages and actions

Timer	Description	Message before expiry	Action after expiry
Router port aging timer	For each router port, the device sets a timer initialized to the aging time of the route port	IGMP general query or PIM hello	The device removes this port from its router port list
Member port aging timer	When a port joins a multicast group, the device sets a timer for the port, which is initialized to the member port aging time	IGMP membership report	The device removes this port from the multicast group forwarding table

Work Mechanism of IGMP Snooping

A device running IGMP Snooping performs different actions when it receives different IGMP messages, as follows:

When receiving a general query

The IGMP querier periodically sends IGMP general queries to all hosts and routers on the local subnet to find out whether active multicast group members exist on the subnet.

Upon receiving an IGMP general query, the device forwards it through all ports in the VLAN except the receiving port and performs the following to the receiving port:

- If the receiving port is a router port existing in its router port list, the device resets the aging timer of this router port.
- If the receiving port is not a router port existing in its router port list, the device adds it into its router port list and sets an aging timer for this router port.

When receiving a membership report

A host sends an IGMP report to the multicast router in the following circumstances:

- Upon receiving an IGMP query, a multicast group member host responds with an IGMP report.
- When intended to join a multicast group, a host sends an IGMP report to the multicast router to announce that it is interested in the multicast information addressed to that group.

Upon receiving an IGMP report, the device forwards it through all the router ports in the VLAN, resolves the address of the multicast group the host is interested in, and performs the following to the receiving port:

- If the port is already in the forwarding table, the device resets the member port aging timer of the port.
- If the port is not in the forwarding table, the device installs an entry for this port in the forwarding table and starts the member port aging timer of this port.



Note

A device will not forward an IGMP report through a non-router port for the following reason: Due to the IGMP report suppression mechanism, if member hosts of that multicast group still exist under non-router ports, the hosts will stop sending reports when they receive the message, and this prevents the device from knowing if members of that multicast group are still attached to these ports.

When receiving a leave message

When an IGMPv1 host leaves a multicast group, the host does not send an IGMP leave message, so the device cannot know immediately that the host has left the multicast group. However, as the host stops sending IGMP reports as soon as it leaves a multicast group, the device deletes the forwarding entry for the member port corresponding to the host from the forwarding table when its aging timer expires.

When an IGMPv2 or IGMPv3 host leaves a multicast group, the host sends an IGMP leave message to the multicast router to announce that it has leaf the multicast group.

Upon receiving an IGMP leave message on the last member port, a device forwards it out all router ports in the VLAN. Because the device does not know whether any other member hosts of that multicast group still exists under the port to which the IGMP leave message arrived, the device does not

immediately delete the forwarding entry corresponding to that port from the forwarding table; instead, it resets the aging timer of the member port.

Upon receiving the IGMP leave message from a host, the IGMP querier resolves from the message the address of the multicast group that the host just left and sends an IGMP group-specific query to that multicast group through the port that received the leave message. Upon receiving the IGMP group-specific query, a device forwards it through all the router ports in the VLAN and all member ports of that multicast group, and performs the following to the receiving port:

- If any IGMP report in response to the group-specific query arrives to the member port before its aging timer expires, this means that some other members of that multicast group still exist under that port: the device resets the aging timer of the member port.
- If no IGMP report in response to the group-specific query arrives to the member port before its aging timer expires as a response to the IGMP group-specific query, this means that no members of that multicast group still exist under the port: the device deletes the forwarding entry corresponding to the port from the forwarding table when the aging timer expires.

Caution

After a device enables IGMP Snooping, when it receives the IGMP leave message sent by a host in a multicast group, it judges whether the multicast group exists automatically. If the multicast group does not exist, the device drops this IGMP leave message.

IGMP Snooping Configuration

IGMP Snooping Configuration Task List

Complete the following tasks to configure IGMP Snooping:

Operation	Remarks
Enabling IGMP Snooping	Required
Configuring the Version of IGMP Snooping	Optional
Configuring Timers	Optional
Configuring Fast Leave Processing	Optional
Configuring a Multicast Group Filter	Optional
Configuring the Maximum Number of Multicast Groups on a Port	Optional
Configuring IGMP Querier	Optional
Suppressing Flooding of Unknown Multicast Traffic in a VLAN	Optional
Configuring Static Member Port for a Multicast Group	Optional
Configuring a Static Router Port	Optional
Configuring a Port as a Simulated Group Member	Optional

Operation	Remarks
Configuring a VLAN Tag for Query Messages	Optional
Configuring Multicast VLAN	Optional

Enabling IGMP Snooping

Follow these steps to enable IGMP Snooping:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable IGMP Snooping globally	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled globally.
Enter VLAN view	**vlan** *vlan-id*	—
Enable IGMP Snooping on the VLAN	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled on all the VLANs.

Caution

- Before enabling IGMP Snooping in a VLAN, be sure to enable IGMP Snooping globally in system view; otherwise the IGMP Snooping settings will not take effect.
- If IGMP Snooping and VLAN VPN are enabled on a VLAN at the same time, IGMP queries are likely to fail to pass the VLAN. You can solve this problem by configuring VLAN tags for queries. For details, see Configuring a VLAN Tag for Query Messages.

Configuring the Version of IGMP Snooping

With the development of multicast technologies, IGMPv3 has found increasingly wide application. In IGMPv3, a host can not only join a specific multicast group but also explicitly specify to receive or reject the information from a specific multicast source. Working with PIM-SSM, IGMPv3 enables hosts to join specific multicast sources and groups directly, greatly simplifying multicast routing protocols and optimizing the network topology.

Follow these steps to configure the version of IGMP Snooping:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	—
Configure the version of IGMP Snooping	**igmp-snooping version** *version-number*	Optional The default IGMP Snooping version is version 2.

Caution

- Before configuring related IGMP Snooping functions, you must enable IGMP Snooping in the specified VLAN.
- Different multicast group addresses should be configured for different multicast sources because IGMPv3 Snooping cannot distinguish multicast data from different sources to the same multicast group.

Configuring Timers

This section describes how to configure the aging timer of the router port, the aging timer of the multicast member ports, and the query response timer.

Follow these steps to configure timers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the aging timer of the router port	**igmp-snooping router-aging-time** *seconds*	Optional By default, the aging time of the router port is 105 seconds.
Configure the query response timer	**igmp-snooping max-response-time** *seconds*	Optional By default, the query response timeout time is 10 seconds.
Configure the aging timer of the multicast member port	**igmp-snooping host-aging-time** *seconds*	Optional By default, the aging time of multicast member ports is 260 seconds

Configuring Fast Leave Processing

With fast leave processing enabled, when the device receives an IGMP leave message on a port, the device directly removes that port from the forwarding table entry for the specific group. If only one host is attached to the port, enable fast leave processing to improve bandwidth management.

Enabling fast leave processing in system view

Follow these steps to enable fast leave processing in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable fast leave processing	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	Required By default, the fast leave processing feature is disabled.

Enabling fast leave processing in Ethernet port view

Follow these steps to enable fast leave processing in Ethernet view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable fast leave processing for specific VLANs	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	Required By default, the fast leave processing feature is disabled.

Note

- The fast leave processing function works for a port only if the host attached to the port runs IGMPv2 or IGMPv3.
- The configuration performed in system view takes effect on all ports of the device if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on all ports in the specified VLAN(s).
- The configuration performed in Ethernet port view takes effect on the port no matter which VLAN it belongs to if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on the port only if the port belongs to the specified VLAN(s).
- If fast leave processing and unknown multicast packet dropping are enabled on a port to which more than one host is connected, when one host leaves a multicast group, the other hosts connected to port and interested in the same multicast group will fail to receive multicast data for that group.

Configuring a Multicast Group Filter

On an IGMP Snooping-enabled device, the configuration of a multicast group allows the service provider to define restrictions on multicast programs available to different users.

In an actual application, when a user requests a multicast program, the user's host initiates an IGMP report. Upon receiving this report message, the device checks the report against the ACL rule configured on the receiving port. If the receiving port can join this multicast group, the device adds this port to the IGMP Snooping multicast group list; otherwise the device drops this report message. Any multicast data that has failed the ACL check will not be sent to this port. In this way, the service provider can control the VOD programs provided for multicast users.

Make sure that an ACL rule has been configured before configuring this feature.

Configuring a multicast group filter in system view

Follow these steps to configure a multicast group filter in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a multicast group filter	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	Required No group filter is configured by default, namely hosts can join any multicast group.

Configuring a multicast group filter in Ethernet port view

Follow these steps to configure a multicast group filter in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure a multicast group filter	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	Optional No group filter is configured by default, namely hosts can join any multicast group.

Note

- A port can belong to multiple VLANs, you can configure only one ACL rule per VLAN on a port.
- If no ACL rule is configured, all the multicast groups will be filtered.
- Since most devices broadcast unknown multicast packets by default, this function is often used together with the function of dropping unknown multicast packets to prevent multicast streams from being broadcast as unknown multicast packets to a port blocked by this function.
- The configuration performed in system view takes effect on all ports of the device if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on all ports in the specified VLAN(s).
- The configuration performed in Ethernet port view takes effect on the port no matter which VLAN it belongs to if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on the port only if the port belongs to the specified VLAN(s).

Configuring the Maximum Number of Multicast Groups on a Port

By configuring the maximum number of multicast groups that can be joined on a port, you can limit the number of multicast programs on-demand available to users, thus to regulate traffic on the port.

Follow these steps to configure the maximum number of multicast groups on a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Limit the number of multicast groups on a port	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list* [**overflow-replace**]]	Required The system default for the device is 256.

Note

- To prevent bursting traffic in the network or performance deterioration of the device caused by excessive multicast groups, you can set the maximum number of multicast groups that the device should process.
- When the number of multicast groups exceeds the configured limit, the device removes its multicast forwarding entries starting from the oldest one. In this case, the multicast packets for the removed multicast group(s) will be flooded in the VLAN as unknown multicast packets. As a result, non-member ports can receive multicast packets within a period of time. To avoid this from happening, enable the function of dropping unknown multicast packets.

Configuring IGMP Querier

In an IP multicast network running IGMP, a multicast router or Layer 3 multicast device is responsible for sending IGMP general queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries, thus to forward multicast traffic correctly at the network layer. This router or Layer 3 device is called IGMP querier.

However, a Layer 2 multicast device does not support IGMP, and therefore cannot send general queries by default. By enabling IGMP Snooping on a Layer 2 device in a VLAN where multicast traffic needs to be Layer-2 switched only and no multicast routers are present, the Layer 2 device will act as the IGMP Snooping querier to send IGMP general queries, thus allowing multicast forwarding entries to be established and maintained at the data link layer.

You can also configure the source address, maximum response time and interval of general queries to be sent from the IGMP Snooping querier.

Follow these steps to configure IGMP Snooping querier:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable IGMP Snooping	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled.
Enter VLAN view	**vlan** vlan-id	—
Enable IGMP Snooping	**igmp-snooping enable**	Required.

To do…	Use the command…	Remarks
Enable IGMP Snooping querier	**igmp-snooping querier**	Required By default, IGMP Snooping querier is disabled.
Configure the interval of sending general queries	**igmp-snooping query-interval** *seconds*	Optional By default, the interval of sending general queries is 60 seconds.
Configure the source IP address of general queries	**igmp-snooping general-query source-ip** { **current-interface** | *ip-address* }	Optional By default, the source IP address of general queries is 0.0.0.0.

Suppressing Flooding of Unknown Multicast Traffic in a VLAN

With IGMP Snooping enabled in a VLAN, multicast traffic for unknown multicast groups is flooded within the VLAN by default. This wastes network bandwidth and affects multicast forwarding efficiency.

With the unknown multicast flooding suppression function enabled, when receiving a multicast packet for an unknown multicast group, an IGMP Snooping device creates a nonflooding entry and relays the packet to router ports only, instead of flooding the packet within the VLAN. If the device has no router ports, it drops the multicast packet.

Follow these steps to suppress flooding of unknown multicast traffic in the VLAN:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable unknown multicast flooding suppression	**igmp-snooping nonflooding-enable**	Required By default, unknown multicast flooding suppression

Note

If the function of dropping unknown multicast packets is enabled, you cannot enable unknown multicast flooding suppression.

Configuring Static Member Port for a Multicast Group

If the host connected to a port is interested in the multicast data for a specific group, you can configure that port as a static member port for that multicast group.

In Ethernet port view

Follow these steps to configure a static multicast group member port in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the current port as a static member port for a multicast group in a VLAN	**multicast static-group** *group-address* **vlan** *vlan-id*	Required By default, no port is configured as a static multicast group member port.

In VLAN interface view

Follow these steps to configure a static multicast group member port in VLAN interface view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface vlan-interface** *interface-number*	—
Configure specified port(s) as static member port(s) of a multicast group in the VLAN	**multicast static-group** *group-address* **interface** *interface-list*	Required By default, no port is configured as a static multicast group member port.

Configuring a Static Router Port

In a network where the topology is unlikely to change, you can configure a port on the device as a static router port, so that the device has a static connection to a multicast router and receives IGMP messages from that router.

In Ethernet port view

Follow these steps to configure a static router port in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the current port as a static router port	**multicast static-router-port vlan** *vlan-id*	Required By default, no static router port is configured.

In VLAN view

Follow these steps to configure a static router port in VLAN view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	—
Configure a specified port as a static router port	**multicast static-router-port** *interface-type interface-number*	Required By default, no static router port is configured.

Configuring a Port as a Simulated Group Member

Generally, hosts running IGMP respond to the IGMP query messages of the multicast device. If hosts fail to respond for some reason, the multicast device may consider that there is no member of the multicast group on the local subnet and remove the corresponding path.

To avoid this from happening, you can configure a port of the VLAN of the device as a multicast group member. When the port receives IGMP query messages, the multicast device will respond. As a result, the port of the VLAN can continue to receive multicast traffic.

Through this configuration, the following functions can be implemented:

- When an Ethernet port is configured as a simulated member host, the device sends an IGMP report through this port. Meanwhile, the device sends the same IGMP report to itself and establishes a corresponding IGMP entry based on this report.
- When receiving an IGMP general query, the simulated host responds with an IGMP report. Meanwhile, the device sends the same IGMP report to itself to ensure that the IGMP entry does not age out.
- When the simulated joining function is disabled on an Ethernet port, the simulated host sends an IGMP leave message.

Therefore, to ensure that IGMP entries will not age out, the port must receive IGMP general queries periodically.

Follow these steps to configure a port as a simulated group member:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the current port as a simulated multicast group member	**igmp host-join** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	Optional Simulated joining is disabled by default.

Caution

- Before configuring a simulated host, enable IGMP Snooping in VLAN view first.
- The port to be configured must belong to the specified VLAN; otherwise the configuration does not take effect.
- You can use the **source-ip** *source-address* command to specify a multicast source address that the port will join as a simulated host. This configuration takes effect when IMGPv3 Snooping is enabled in the VLAN.

Configuring a VLAN Tag for Query Messages

By configuring the VLAN tag carried in IGMP general and group-specific queries forwarded and sent by IGMP Snooping devices and by configuring the VLAN mapping function, you can enable multicast packet forwarding between different VLANs In a Layer-2 multicast network environment.

For description about VLAN mapping, see “QoS-QoS Profile”.

Follow these steps to configure VLAN Tag for query message:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable IGMP Snooping	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled.
Configure a VLAN tag for query messages	**igmp-snooping vlan-mapping vlan** *vlan-id*	Required By default, no VLAN tag is configured for general and group-specific query messages sent or forwarded by IGMP Snooping.

Configuring Multicast VLAN

In traditional multicast implementations, when users in different VLANs listen to the same multicast group, the multicast data is copied on the multicast router for each VLAN that contains receivers. This is a big waste of network bandwidth.

In an IGMP Snooping environment, by configuring a multicast VLAN and adding ports to the multicast VLAN, you can allow users in different VLANs to share the same multicast VLAN. This saves bandwidth because multicast streams are transmitted only within the multicast VLAN. In addition, because the multicast VLAN is isolated from user VLANs, this method also enhances the information security.

Multicast VLAN is mainly used in Layer 2 switching, but you must make the corresponding configurations on the Layer 3 device.

Follow these steps to configure multicast VLAN on the Layer 3 device:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a multicast VLAN and enter VLAN view	**vlan** *vlan-id*	—
Return to system view	**quit**	—

To do…	Use the command…	Remarks
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Enable IGMP	**igmp enable**	Required By default, the IGMP feature is disabled.
Return to system view	**quit**	—
Enter Ethernet port view for the Layer 2 device to be configured	**interface** *interface-type interface-number*	—
Define the port as a trunk or hybrid port	**port link-type** { **trunk** | **hybrid** }	Required
Specify the VLANs to be allowed to pass the Ethernet port	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Required The multicast VLAN defined on the Layer 2 device must be included, and the port must be configured to forward tagged packets for the multicast VLAN if the port type is hybrid.
	port trunk permit vlan *vlan-list*	

Follow these steps to configure multicast VLAN on the Layer 2 device:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable IGMP Snooping	**igmp-snooping enable**	—
Enter VLAN view	**vlan** vlan-id	—
Enable IGMP Snooping	**igmp-snooping enable**	Required
Enable multicast VLAN	**service-type multicast**	Required
Return to system view	**quit**	—
Enter Ethernet port view for the Layer 3 device	**interface** *interface-type interface-number*	—
Define the port as a trunk or hybrid port	**port link-type** { **trunk** | **hybrid** }	Required
Specify the VLANs to be allowed to pass the Ethernet port	**port hybrid vlan** *vlan-list* { **tagged** | **untagged** }	Required The multicast VLAN must be included, and the port must be configured to forward tagged packets for the multicast VLAN if the port type is hybrid.
	port trunk permit vlan *vlan-list*	
Enter Ethernet port view for a user device	**interface** *interface-type interface-number*	—
Define the port as a hybrid port	**port link-type hybrid**	Required
Specify the VLANs to be allowed to pass the port	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Required The multicast VLAN must be included, and the port must be configured to forward tagged packets for the multicast VLAN.

Note

- One port can belong to only one multicast VLAN.
- The port connected to a user terminal must be a hybrid port.
- The multicast member ports must be in the same VLAN with the router port. Otherwise, the multicast member port cannot receive multicast packets.
- If a router port is in a multicast VLAN, the router port must be configured as a trunk port or a hybrid port that allows tagged packets to pass for the multicast VLAN. Otherwise, all the multicast member ports in this multicast VLAN cannot receive multicast packets.
- When the multicast VLAN is set up, all IGMP report messages are forwarded to the router ports in the multicast VLAN. If no router ports exist in the multicast VLAN, all IGMP report messages are flooded within the multicast VLAN.

Displaying and Maintaining IGMP Snooping

To do…	Use the command…	Remarks
Display the current IGMP Snooping configuration	**display igmp-snooping configuration**	Available in any view
Display IGMP Snooping message statistics	**display igmp-snooping statistics**	
Display the information about IP and MAC multicast groups in one or all VLANs	**display igmp-snooping group** [**vlan** *vlanid*]	
Clear IGMP Snooping statistics	**reset igmp-snooping statistics**	Available in user view

IGMP Snooping Configuration Examples

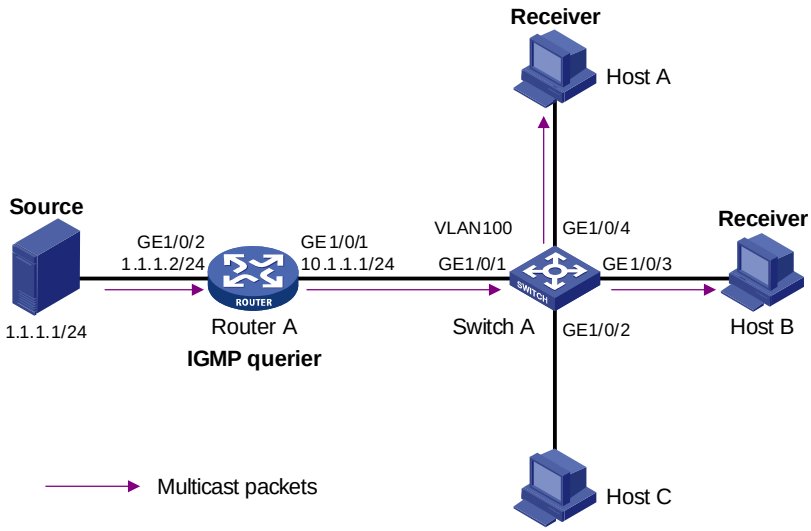
Configuring IGMP Snooping

Network requirements

To prevent multicast traffic from being flooded at Layer 2, enable IGMP Snooping on Layer 2 devices.

- As shown in Figure 2-3, Router A connects to a multicast source (Source) through GigabitEthernet1/0/2, and to Switch A through GigabitEthernet1/0/1.
- Run PIM-DM and IGMP on Router A. Run IGMP snooping on Switch A. Router A acts as the IGMP querier.
- The multicast source sends multicast data to the multicast group 224.1.1.1. Host A and Host B are receivers of the multicast group 224.1.1.1.

Figure 2-3 Network diagram for IGMP Snooping configuration



Configuration procedure

1) Configure the IP address of each interface

Configure an IP address and subnet mask for each interface as per Figure 2-3. The detailed configuration steps are omitted.

2) Configure Router A

Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on GigabitEthernet1/0/1.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface GigabitEthernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface GigabitEthernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

3) Configure Switch A

Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
  Enable IGMP-Snooping ok.
```

Create VLAN 100, assign GigabitEthernet1/0/1 through GigabitEthernet1/0/4 to this VLAN, and enable IGMP Snooping in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

4) Verify the configuration

View the detailed information of the multicast group in VLAN 100 on Switch A.

```
<SwitchA> display igmp-snooping group vlan100
```

```
Total 1 IP Group(s).
Total 1 MAC Group(s).

Vlan(id):100.
  Total 1 IP Group(s).
  Total 1 MAC Group(s).
  Static Router port(s):
  Dynamic Router port(s):
                  GigabitEthernet1/0/1
  IP group(s):the following ip group(s) match to one mac group.
      IP group address: 224.1.1.1
      Static host port(s):
      Dynamic host port(s):
                  GigabitEthernet1/0/3          GigabitEthernet1/0/4
  MAC group(s):
      MAC group address: 0100-5e01-0101
      Host port(s):GigabitEthernet1/0/3          GigabitEthernet1/0/4
```

As shown above, the multicast group 224.1.1.1 is established on Switch A, with the dynamic router port GigabitEthernet1/0/1 and dynamic member ports GigabitEthernet1/0/3 and GigabitEthernet1/0/4. This means that Host A and Host B have joined the multicast group 224.1.1.1.

Configuring Multicast VLAN

Network requirements

As shown in Figure 2-4, Workstation is a multicast source. Switch A forwards multicast data from the multicast source. A Layer 2 device, Switch B forwards the multicast data to the end users Host A and Host B.

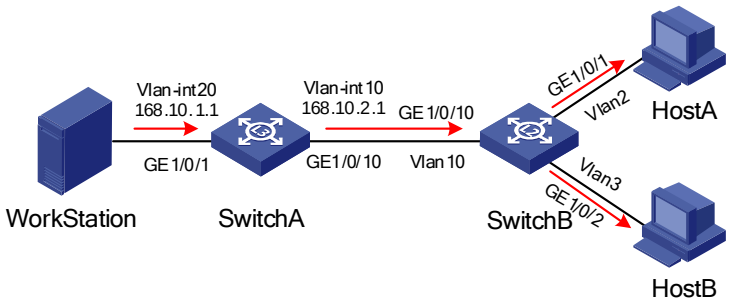
Table 2-2 describes the network devices involved in this example and the configurations you should make on them.

Table 2-2 Network devices and their configurations

Device	Device description	Networking description
Switch A	Layer 3 device	The interface IP address of VLAN 20 is 168.10.1.1. GigabitEthernet 1/0/1 is connected to the workstation and belongs to VLAN 20. The interface IP address of VLAN 10 is 168.10.2.1. GigabitEthernet 1/0/10 belongs to VLAN 10. GigabitEthernet 1/0/10 is connected to Switch B.
Switch B	Layer 2 device	VLAN 2 contains GigabitEthernet 1/0/1 and VLAN 3 contains GigabitEthernet 1/0/2. The two ports are connected to Host A and Host B, respectively. VLAN 10 includes GigabitEthernet 1/0/10, GigabitEthernet1/0/1, and GigabitEthernet 1/0/2. GigabitEthernet 1/0/10 is connected to Switch A. VLAN 10 is a multicast VLAN.
Host A	User 1	Host A is connected to GigabitEthernet 1/0/1 on Switch B.
Host B	User 2	Host B is connected to GigabitEthernet 1/0/2 on Switch B.

Configure a multicast VLAN, so that users in VLAN 2 and VLAN 3 can receive multicast streams through the multicast VLAN.

Figure 2-4 Network diagram for multicast VLAN configuration



Configuration procedure

The following configuration is based on the prerequisite that the devices are properly connected and all the required IP addresses are already configured.

1) Configure Switch A:

Set the interface IP address of VLAN 20 to 168.10.1.1 and enable PIM DM on the VLAN interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] vlan 20
[SwitchA–vlan20]port GigabitEthernet 1/0/1
[SwitchA-vlan20] quit
[SwitchA] interface Vlan-interface 20
[SwitchA-Vlan-interface20] ip address 168.10.1.1 255.255.255.0
[SwitchA-Vlan-interface20] pim dm
[SwitchA-Vlan-interface20] quit
```

Configure VLAN 10.

```
[SwitchA] vlan 10
[SwitchA-vlan10] quit
```

Define GigabitEthernet 1/0/10 as a hybrid port, add the port to VLAN 10, and configure the port to forward tagged packets for VLAN 10.

```
[SwitchA] interface GigabitEthernet 1/0/10
[SwitchA-GigabitEthernet1/0/10] port link-type hybrid
[SwitchA-GigabitEthernet1/0/10] port hybrid vlan 10 tagged
[SwitchA-GigabitEthernet1/0/10] quit
```

Configure the interface IP address of VLAN 10 as 168.10.2.1, and enable PIM-DM and IGMP.

```
[SwitchA] interface Vlan-interface 10
[SwitchA-Vlan-interface10] ip address 168.10.2.1 255.255.255.0
[SwitchA-Vlan-interface10] igmp enable
```

2) Configure Switch B:

Enable the IGMP Snooping feature on Switch B.

```
<SwitchB> system-view
[SwitchB] igmp-snooping enable
```

Configure VLAN 10 as the multicast VLAN and enable IGMP Snooping on it.

```
[SwitchB] vlan 10
[SwitchB-vlan10] service-type multicast
[SwitchB-vlan10] igmp-snooping enable
[SwitchB-vlan10] quit
```

Define GigabitEthernet 1/0/10 as a hybrid port, add the port to VLAN 2, VLAN 3, and VLAN 10, and configure the port to forward tagged packets for VLAN 2, VLAN 3, and VLAN 10.

```
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port link-type hybrid
[SwitchB-GigabitEthernet1/0/10] port hybrid vlan 2 3 10 tagged
[SwitchB-GigabitEthernet1/0/10] quit
```

Define GigabitEthernet 1/0/1 as a hybrid port, add the port to VLAN 2 and VLAN 10, configure the port to forward untagged packets for VLAN 2 and VLAN 10, and set VLAN 2 as the default VLAN of the port.

```
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type hybrid
[SwitchB-GigabitEthernet1/0/1] port hybrid vlan 2 10 untagged
[SwitchB-GigabitEthernet1/0/1] port hybrid pvid vlan 2
[SwitchB-GigabitEthernet1/0/1] quit
```

Define GigabitEthernet 1/0/2 as a hybrid port, add the port to VLAN 3 and VLAN 10, configure the port to forward untagged packets for VLAN 3 and VLAN 10, and set VLAN 3 as the default VLAN of the port.

```
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type hybrid
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 3 10 untagged
[SwitchB-GigabitEthernet1/0/2] port hybrid pvid vlan 3
[SwitchB-GigabitEthernet1/0/2] quit
```

Troubleshooting IGMP Snooping

Symptom: Multicast function does not work on the device.

Solution:

Possible reasons are:

1) IGMP Snooping is not enabled.

- Use the **display current-configuration** command to check the status of IGMP Snooping.
- If IGMP Snooping is disabled, check whether it is disabled globally or in the specific VLAN. If it is disabled globally, use the **igmp-snooping enable** command in both system view and VLAN view to enable it both globally and on the corresponding VLAN at the same time. If it is only disabled on the corresponding VLAN, use the **igmp-snooping enable** command in VLAN view only to enable it on the corresponding VLAN.

2) Multicast forwarding table set up by IGMP Snooping is wrong.

- Use the **display igmp-snooping group** command to check if the multicast groups are expected ones.
- If the multicast group set up by IGMP Snooping is not correct, contact your technical support personnel.

3 Common Multicast Configuration

Common Multicast Configuration

Configuring a Multicast MAC Address Entry

In Layer 2 multicast, the system can add multicast forwarding entries dynamically through a Layer 2 multicast protocol. Alternatively, you can statically bind a port to a multicast MAC address entry by configuring a multicast MAC address entry manually.

Generally, when receiving a multicast packet for a multicast group not yet registered on the device, the device will flood the packet within the VLAN to which the port belongs. You can configure a static multicast MAC address entry to avoid this.

Follow these steps to configure a multicast MAC address entry in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a multicast MAC address entry	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	Required The *mac-address* argument must be a multicast MAC address.

Follow these steps to configure a multicast MAC address entry in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Create a multicast MAC address entry.	**mac-address multicast** *mac-address* **vlan** *vlan-id*	Required The *mac-address* argument must be a multicast MAC address.

Note

- If the multicast MAC address entry to be created already exists, the system gives you a prompt.
- If you want to add a port to a multicast MAC address entry created through the **mac-address multicast** command, you need to remove the entry first, create this entry again, and then add the specified port to the forwarding ports of this entry.
- You cannot enable link aggregation on a port on which you have configured a multicast MAC address, and you cannot configure a multicast MAC address on an aggregation port.
- You cannot configure a multicast MAC address starting with 01005e in an IGMP-Snooping-enabled VLAN. You can do that if IGMP Snooping is not enabled in the VLAN.

Configuring Dropping Unknown Multicast Packets

Generally, if the multicast address of the multicast packet received on the device is not registered on the local device, the packet will be flooded in the VLAN. When the function of dropping unknown multicast packets is enabled, the device will drop any multicast packets whose multicast address is not registered. Thus, the bandwidth is saved and the processing efficiency of the system is improved.

Follow these steps to configure dropping unknown multicast packet:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure dropping unknown multicast packets	**unknown-multicast drop enable**	Required By default, the function of dropping unknown multicast packets is disabled.

Displaying and Maintaining Common Multicast Configuration

To do…	Use the command…	Remarks
Display the created multicast MAC table entries	**display mac-address multicast** [**static** { { { *mac-address* **vlan** *vlan-id* **| vlan** *vlan-id* } [**count**] } | **count** }]	You can execute the **display** commands in any view.

Table of Contents

1 NTP Configuration 1-1
Introduction to NTP 1-1
Applications of NTP 1-1
Implementation Principle of NTP 1-2
NTP Implementation Modes 1-3
NTP Configuration Task List 1-6
Configuring NTP Implementation Modes 1-6
Configuring NTP Server/Client Mode 1-6
Configuring the NTP Symmetric Peer Mode 1-7
Configuring NTP Broadcast Mode 1-8
Configuring NTP Multicast Mode 1-9
Configuring Access Control Right 1-10
Configuration Prerequisites 1-10
Configuration Procedure 1-10
Configuring NTP Authentication 1-10
Configuration Prerequisites 1-11
Configuration Procedure 1-11
Configuring Optional NTP Parameters 1-13
Configuring an Interface on the Local Device to Send NTP Messages 1-13
Configuring the Number of Dynamic Sessions Allowed on the Local Device 1-14
Disabling an Interface from Receiving NTP messages 1-14
Displaying and Maintaining NTP Configuration 1-14
NTP Configuration Examples 1-14
Configuring NTP Server/Client Mode 1-14
Configuring NTP Symmetric Peer Mode 1-16
Configuring NTP Broadcast Mode 1-17
Configuring NTP Multicast Mode 1-19
Configuring NTP Server/Client Mode with Authentication 1-20

1 NTP Configuration

When configuring NTP, go to these sections for information you are interested in:

- Introduction to NTP
- NTP Configuration Task List
- Configuring NTP Implementation Modes
- Configuring Access Control Right
- Configuring NTP Authentication
- Configuring Optional NTP Parameters
- Displaying and Maintaining NTP Configuration
- NTP Configuration Examples

Note

- The term switch used throughout this document refers to a switching device in a generic sense or the switching engine of a WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Introduction to NTP

Network time protocol (NTP) is a time synchronization protocol defined in RFC 1305. It is used for time synchronization between a set of distributed time servers and clients. Carried over UDP, NTP transmits packets through UDP port 123.

NTP is intended for time synchronization between all devices that have clocks in a network so that the clocks of all devices can keep consistent. Thus, the devices can provide multiple unified-time-based applications (See Applications of NTP).

A local system running NTP can not only be synchronized by other clock sources, but also serve as a clock source to synchronize other clocks. Besides, it can synchronize, or be synchronized by other systems by exchanging NTP messages.

Applications of NTP

As setting the system time manually in a network with many devices leads to a lot of workload and cannot ensure accuracy, it is unfeasible for an administrator to perform the operation. However, an administrator can synchronize the clocks of devices in a network with required accuracy by performing NTP configuration.

NTP is mainly applied to synchronizing the clocks of all devices in a network. For example:

- In network management, the analysis of the log information and debugging information collected from different devices is meaningful and valid only when network devices that generate the information adopts the same time.
- The billing system requires that the clocks of all network devices be consistent.
- Some functions, such as restarting all network devices in a network simultaneously require that they adopt the same time.
- When multiple systems cooperate to handle a rather complex transaction, they must adopt the same time to ensure a correct execution order.
- To perform incremental backup operations between a backup server and a host, you must make sure they adopt the same time.

NTP has the following advantages:

- Defining the accuracy of clocks by stratum to synchronize the clocks of all devices in a network quickly
- Supporting access control (See Configuring Access Control Right) and MD5 encrypted authentication (See Configuring NTP Authentication)
- Sending protocol packets in unicast, multicast, or broadcast mode

---

Note

- The clock stratum determines the accuracy, which ranges from 1 to 16. The stratum of a reference clock ranges from 1 to 15. The clock accuracy decreases as the stratum number increases. A stratum 16 clock is in the unsynchronized state and cannot serve as a reference clock.
- The local clock of the device cannot be set as a reference clock. It can serve as a reference clock source to synchronize the clock of other devices only after it is synchronized.

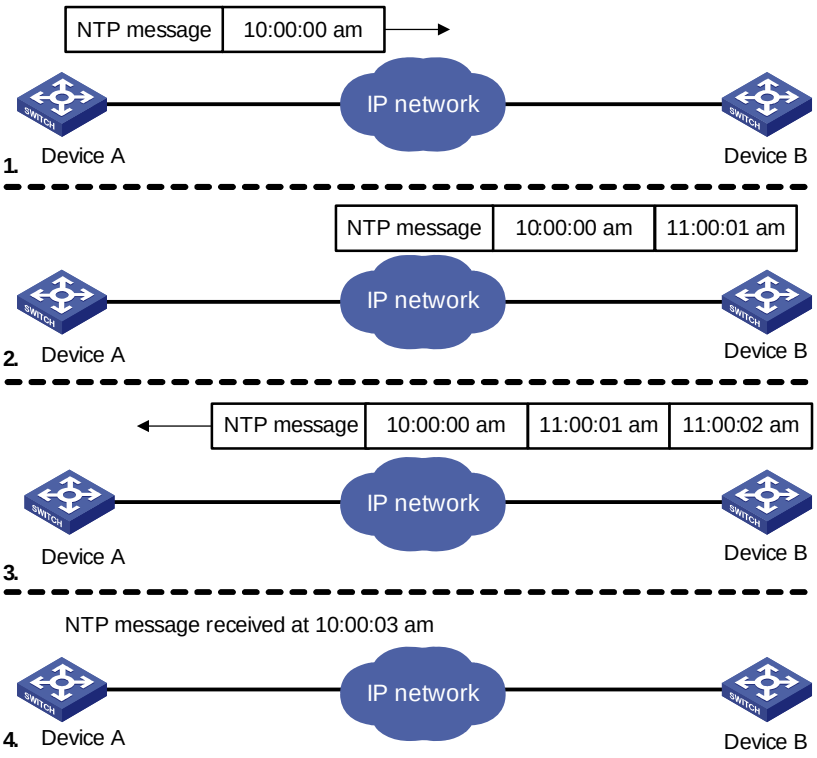
Implementation Principle of NTP

Figure 1-1 shows the implementation principle of NTP.

Device A is connected to Device B through Ethernet ports. Both having their own system clocks, they need to synchronize the clocks of each other through NTP. To help you to understand the implementation principle, we suppose that:

- Before the system clocks of Device A and Device B are synchronized, the clock of Device A is set to 10:00:00 am, and the clock of Device B is set to 11:00:00 am.
- Device B serves as the NTP server, that is, the clock of Device A will be synchronized to that of Device B.
- It takes one second to transfer an NTP message from Device A to Device B or from Device B to Device A.

Figure 1-1 Implementation principle of NTP



The procedure of synchronizing the system clock is as follows:

- Device A sends an NTP message to Device B, with a timestamp 10:00:00 am (T_1) identifying when it is sent.
- When the message arrives at Device B, Device B inserts its own timestamp 11:00:01 am (T_2) into the packet.
- When the NTP message leaves Device B, Device B inserts its own timestamp 11:00:02 am (T_3) into the packet.
- When receiving a response packet, Device A inserts a new timestamp 10:00:03 am (T_4) into it.

At this time, Device A has enough information to calculate the following two parameters:

- Delay for an NTP message to make a round trip between Device A and Device B:

$$Delay = (T_4 - T_1) - (T_3 - T_2).$$

- Time offset of Device A relative to Device B:

$$Offset = ((T_2 - T_1) + (T_3 - T_4))/2.$$

Device A can then set its own clock according to the above information to synchronize its clock to that of Device B.

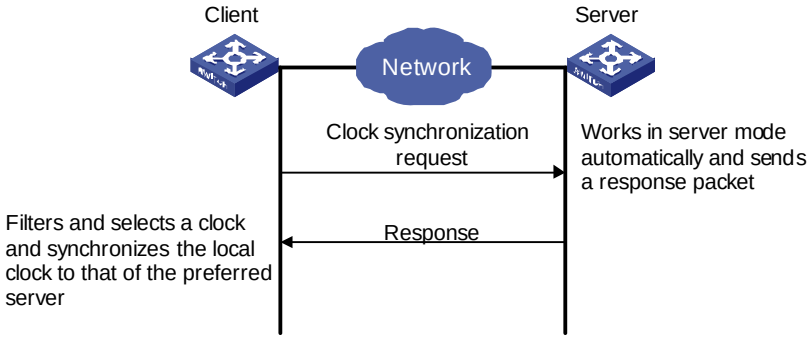
For detailed information, refer to RFC 1305.

NTP Implementation Modes

According to the network structure and the position of the local device in the network, the local Ethernet device can work in multiple NTP modes to synchronize the clock.

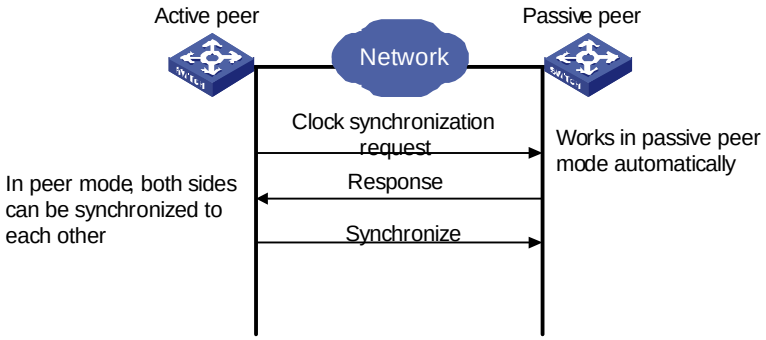
Server/client mode

Figure 1-2 Server/client mode



Symmetric peer mode

Figure 1-3 Symmetric peer mode

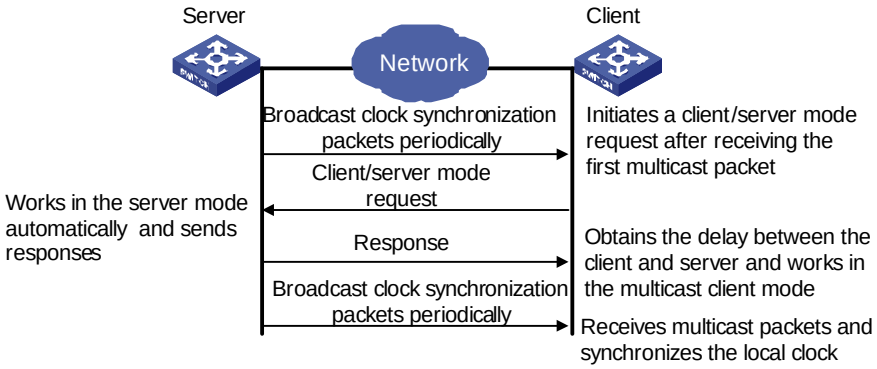


In the symmetric peer mode, the local device serves as the symmetric-active peer and sends clock synchronization request first, while the remote server serves as the symmetric-passive peer automatically.

If both of the peers have reference clocks, the one with a smaller stratum number is adopted.

Broadcast mode

Figure 1-4 Broadcast mode



Multicast mode

Figure 1-5 Multicast mode

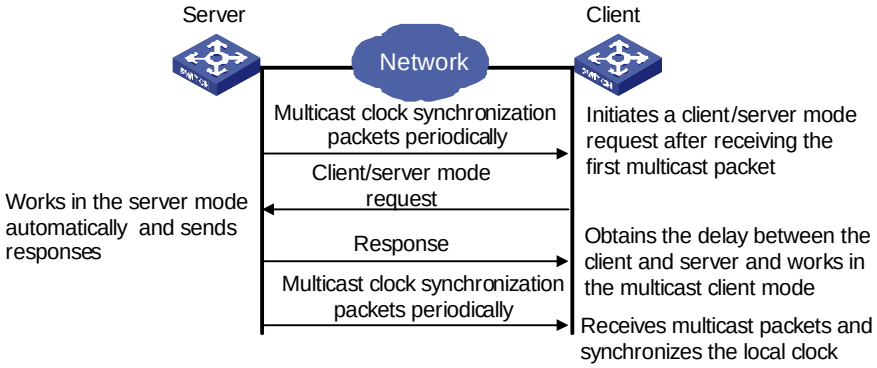


Table 1-1 describes how the above mentioned NTP modes are implemented on the device.

Table 1-1 NTP implementation modes on the device

NTP implementation mode	Configuration on the device
Server/client mode	Configure the local device to work in the NTP client mode. In this mode, the remote server serves as the local time server, while the local device serves as the client.
Symmetric peer mode	Configure the local device to work in NTP symmetric peer mode. In this mode, the remote server serves as the symmetric-passive peer of the device, and the local device serves as the symmetric-active peer.
Broadcast mode	• Configure the local device to work in NTP broadcast server mode. In this mode, the local device broadcasts NTP messages through the VLAN interface configured on the device. • Configure the device to work in NTP broadcast client mode. In this mode, the local device receives broadcast NTP messages through the VLAN interface configured on the device.
Multicast mode	• Configure the local device to work in NTP multicast server mode. In this mode, the local device sends multicast NTP messages through the VLAN interface configured on the device. • Configure the local device to work in NTP multicast client mode. In this mode, the local device receives multicast NTP messages through the VLAN interface configured on the device.

Caution

- When the device works in server mode or symmetric passive mode, you need not to perform related configurations on this device but do that on the client or the symmetric-active peer.
- The NTP server mode, NTP broadcast mode, or NTP multicast mode takes effect only after the local clock of the device has been synchronized.
- When symmetric peer mode is configured on two devices, to synchronize the clock of the two devices, make sure at least one device's clock has been synchronized.

NTP Configuration Task List

Complete the following tasks to configure NTP:

Task	Remarks
Configuring NTP Implementation Modes	Required
Configuring Access Control Right	Optional
Configuring NTP Authentication	Optional
Configuring Optional NTP Parameters	Optional
Displaying and Maintaining NTP Configuration	Optional

Configuring NTP Implementation Modes

The device can work in one of the following NTP modes:

- Configuring NTP Server/Client Mode
- Configuring the NTP Symmetric Peer Mode
- Configuring NTP Broadcast Mode
- Configuring NTP Multicast Mode

 **Note**

To protect unused sockets against attacks by malicious users and improve security, the device provides the following functions:

- UDP port 123 is opened only when the NTP feature is enabled.
- UDP port 123 is closed as the NTP feature is disabled.

These functions are implemented as follows:

- Execution of one of the **ntp-service unicast-server**, **ntp-service unicast-peer**, **ntp-service broadcast-client**, **ntp-service broadcast-server**, **ntp-service multicast-client**, and **ntp-service multicast-server** commands enables the NTP feature and opens UDP port 123 at the same time.
- Execution of the **undo** form of one of the above six commands disables all implementation modes of the NTP feature and closes UDP port 123 at the same time.

Configuring NTP Server/Client Mode

For devices working in the server/client mode, you only need to perform configurations on the clients, and not on the servers.

Follow these steps to configure an NTP client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure an NTP client	**ntp-service unicast-server** { *remote-ip* | *server-name* } [**authentication-keyid** *key-id* | **priority** | **source-interface Vlan-interface** *vlan-id* | **version** *number*]*	Required By default, the device is not configured to work in the NTP client mode.

Note

- The remote server specified by *remote-ip* or *server-name* serves as the NTP server, and the local device serves as the NTP client. The clock of the NTP client will be synchronized by but will not synchronize that of the NTP server.
- *remote-ip* cannot be a broadcast address, a multicast address or the IP address of the local clock.
- After you specify an interface for sending NTP messages through the **source-interface** keyword, the source IP address of the NTP message will be configured as the primary IP address of the specified interface.
- The device can act as a server to synchronize the clock of other devices only after its clock has been synchronized. If the clock of a server has a stratum level lower than or equal to that of a client's clock, the client will not synchronize its clock to the server's.
- You can configure multiple servers by repeating the **ntp-service unicast-server** command. The client will choose the optimal reference source.

Configuring the NTP Symmetric Peer Mode

For devices working in the symmetric peer mode, you need to specify a symmetric-passive peer on the symmetric-active peer.

Follow these steps to configure a symmetric-active switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify a symmetric-passive peer for the device	**ntp-service unicast-peer** { *remote-ip* | *peer-name* } [**authentication-keyid** *key-id* | **priority** | **source-interface Vlan-interface** *vlan-id* | **version** *number*]*	Required By default, the device is not configured to work in the symmetric mode.

Note

- In the symmetric peer mode, you need to execute the related NTP configuration commands (refer to Configuring NTP Implementation Modes for details) to enable NTP on a symmetric-passive peer; otherwise, the symmetric-passive peer will not process NTP messages from the symmetric-active peer.
- The remote device specified by *remote-ip* or *peer-name* serves as the peer of the local device, and the local device works in the symmetric-active mode. In this case, the clock of the local device and that of the remote device can be synchronized to each other.
- *remote-ip* must not be a broadcast address, a multicast address or the IP address of the local clock.
- After you specify an interface for sending NTP messages through the **source-interface** keyword, the source IP address of the NTP message will be configured as the IP address of the specified interface.
- Typically, the clock of at least one of the symmetric-active and symmetric-passive peers should be synchronized first; otherwise the clock synchronization will not proceed.
- You can configure multiple symmetric-passive peers for the local device by repeating the **ntp-service unicast-peer** command. The clock of the peer with the smallest stratum will be chosen to synchronize with the local clock of the device.

Configuring NTP Broadcast Mode

For devices working in the broadcast mode, you need to configure both the server and clients. The broadcast server periodically sends NTP broadcast messages to the broadcast address 255.255.255.255. The devices working in the NTP broadcast client mode will respond to the NTP messages, so as to start the clock synchronization.

The device can work as a broadcast server or a broadcast client.

Note

A broadcast server can synchronize broadcast clients only after its clock has been synchronized.

Configuring the device to work in the NTP broadcast server mode

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Configure the device to work in the NTP broadcast server mode	**ntp-service broadcast-server** [**authentication-keyid** *key-id* | **version** *number*]*	Required Not configured by default.

Configuring the device to work in the NTP broadcast client mode

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Configure the device to work in the NTP broadcast client mode	**ntp-service broadcast-client**	Required Not configured by default.

Configuring NTP Multicast Mode

For devices working in the multicast mode, you need to configure both the server and clients. The multicast server periodically sends NTP multicast messages to multicast clients. The devices working in the NTP multicast client mode will respond to the NTP messages, so as to start the clock synchronization.

The device can work as a multicast server or a multicast client.

Note

- A multicast server can synchronize multicast clients only after its clock has been synchronized.
- The device working in the multicast server mode supports up to 1,024 multicast clients.

Configuring the device to work in the multicast server mode

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Configure the device to work in the NTP multicast server mode	**ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*]*	Required Not configured by default.

Configuring the device to work in the multicast client mode

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Configure the device to work in the NTP multicast client mode	**ntp-service multicast-client** [*ip-address*]	Required Not configured by default.

Configuring Access Control Right

With the following command, you can configure the NTP service access-control right to the local device for a peer device. There are four access-control rights, as follows:

- **query**: Control query right. This level of right permits the peer device to perform control query to the NTP service on the local device but does not permit the peer device to synchronize its clock to the local device. The so-called “control query” refers to query of state of the NTP service, including alarm information, authentication status, clock source information, and so on.
- **synchronization**: Synchronization right. This level of right permits the peer device to synchronize its clock to the local device but does not permit the peer device to perform control query.
- **server**: Server right. This level of right permits the peer device to perform synchronization and control query to the local device but does not permit the local device to synchronize its clock to the peer device.
- **peer**: Peer access. This level of right permits the peer device to perform synchronization and control query to the local device and also permits the local device to synchronize its clock to the peer device.

From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it will perform an access-control right match in this order and use the first matched right.

Configuration Prerequisites

Prior to configuring the NTP service access-control right to the local device for peer devices, you need to create and configure an ACL associated with the access-control right. For the configuration of ACL, refer to *ACL Configuration* in *Security Volume*.

Configuration Procedure

Follow these steps to configure the NTP service access-control right to the local device for peer devices:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the NTP service access-control right to the local device for peer devices	**ntp-service access** { **peer** | **server** | **synchronization** | **query** } *acl-number*	Optional **peer** by default

Note

The access-control right mechanism provides only a minimum degree of security protection for the local device. A more secure method is identity authentication.

Configuring NTP Authentication

In networks with higher security requirements, the NTP authentication function must be enabled to run NTP. Through password authentication on the client and the server, the clock of the client is

synchronized only to that of the server that passes the authentication. This improves network security. Table 1-2 shows the roles of devices in the NTP authentication function.

Table 1-2 Description on the roles of devices in NTP authentication function

Role of device	Working mode
Client	Client in the server/client mode
	Client in the broadcast mode
	Client in the multicast mode
	Symmetric-active peer in the symmetric peer mode
Server	Server in the server/client mode
	Server in the broadcast mode
	Server in the multicast mode
	Symmetric-passive peer in the symmetric peer mode

Configuration Prerequisites

NTP authentication configuration involves:

- Configuring NTP authentication on the client
- Configuring NTP authentication on the server

Observe the following principles when configuring NTP authentication:

- If the NTP authentication function is not enabled on the client, the clock of the client can be synchronized to a server no matter whether the NTP authentication function is enabled on the server (assuming that other related configurations are properly performed).
- For the NTP authentication function to take effect, a trusted key needs to be configured on both the client and server after the NTP authentication is enabled on them.
- The local clock of the client is only synchronized to the server that provides a trusted key.
- In addition, for the server/client mode and the symmetric peer mode, you need to associate a specific key on the client (the symmetric-active peer in the symmetric peer mode) with the corresponding NTP server (the symmetric-passive peer in the symmetric peer mode); for the NTP broadcast/multicast mode, you need to associate a specific key on the broadcast/multicast server with the corresponding NTP broadcast/multicast client. Otherwise, NTP authentication cannot be enabled normally.
- Configurations on the server and the client must be consistent.

Configuration Procedure

Configuring NTP authentication on the client

Follow these steps to configure NTP authentication on the client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the NTP authentication function	**ntp-service authentication enable**	Required Disabled by default.

To do…		Use the command…	Remarks
Configure the NTP authentication key		**ntp-service authentication-keyid** *key-id* **authentication-model md5** *value*	Required By default, no NTP authentication key is configured.
Configure the specified key as a trusted key		**ntp-service reliable authentication-keyid** *key-id*	Required By default, no trusted key is configured.
Associate the specified key with the corresponding NTP server	Configure on the client in the server/client mode	**ntp-service unicast-server** { *remote-ip* | *server-name* } **authentication-keyid** *key-id*	Required For the client in the NTP broadcast/multicast mode, you just need to associate the specified key with the client on the corresponding server.
	Configure on the symmetric-active peer in the symmetric peer mode	**ntp-service unicast-peer** { *remote-ip* | *peer-name* } **authentication-keyid** *key-id*	

Note

- NTP authentication requires that the authentication keys configured for the server and the client be the same. Besides, the authentication keys must be trusted keys. Otherwise, the clock of the client cannot be synchronized with that of the server.
- In NTP server mode and NTP peer mode, you need to associate the specified key with the corresponding NTP server (symmetric-active peer) on the client (symmetric-passive peer). In these two modes, multiple NTP servers (symmetric-active peers) may be configured for a client/passive peer, and therefore, the authentication key is required to determine which NTP server the local clock is synchronized to.

Configuring NTP authentication on the server

Follow these steps to configure NTP authentication on the server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable NTP authentication	**ntp-service authentication enable**	Required Disabled by default.
Configure an NTP authentication key	**ntp-service authentication-keyid** *key-id* **authentication-mode md5** *value*	Required By default, no NTP authentication key is configured.
Configure the specified key as a trusted key	**ntp-service reliable authentication-keyid** *key-id*	Required By default, no trusted authentication key is configured.
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—

To do…		Use the command…	Remarks
Associate the specified key with the corresponding broadcast/multicast client	Configure on the NTP broadcast server	**ntp-service broadcast-server authentication-keyid** *key-id*	• In NTP broadcast server mode and NTP multicast server mode, you need to associate the specified key with the corresponding broadcast/multicast client • You can associate an NTP broadcast/multicast client with an authentication key while configuring NTP mode. You can also use this command to associate them after configuring the NTP mode.
	Configure on the NTP multicast server	**ntp-service multicast-server authentication-keyid** *key-id*	

Note

The procedure for configuring NTP authentication on the server is the same as that on the client. Besides, the client and the server must be configured with the same authentication key.

Configuring Optional NTP Parameters

Complete the following tasks to configure optional NTP parameters:

Task	Remarks
Configuring an Interface on the Local Device to Send NTP Messages	Optional
Configuring the Number of Dynamic Sessions Allowed on the Local Device	Optional
Disabling an Interface from Receiving NTP messages	Optional

Configuring an Interface on the Local Device to Send NTP Messages

Follow these steps to configure an interface on the local device to send NTP messages:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure an interface on the local device to send NTP messages	**ntp-service source-interface Vlan-interface** *vlan-id*	Required

Caution

If you have specified an interface in the **ntp-service unicast-server** or **ntp-service unicast-peer** command, this interface will be used for sending NTP messages.

Configuring the Number of Dynamic Sessions Allowed on the Local Device

Follow these steps to configure the number of dynamic sessions allowed on the local device:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the maximum number of dynamic sessions that can be established on the local device	**ntp-service max-dynamic-sessions** *number*	Required By default, up to 100 dynamic sessions can be established locally.

Disabling an Interface from Receiving NTP messages

Follow these steps to disable an interface from receiving NTP messages:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Disable an interface from receiving NTP messages	**ntp-service in-interface disable**	Required By default, a VLAN interface receives NTP messages.

Displaying and Maintaining NTP Configuration

To do…	Use the command…	Remarks
Display the status of NTP services	**display ntp-service status**	Available in any view
Display the information about the sessions maintained by NTP	**display ntp-service sessions** [**verbose**]	
Display the brief information about NTP servers along the path from the local device to the reference clock source	**display ntp-service trace**	

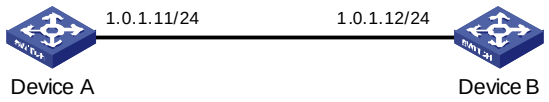
NTP Configuration Examples

Configuring NTP Server/Client Mode

Network requirements

- As shown in Figure 1-6, the local clock of Device A is to be used as a master clock, with the stratum level of 2.
- Device A is used as the NTP server of Device B (a WX3000 series device)
- Configure Device B to work in the client mode, and then Device A will automatically work in the server mode.

Figure 1-6 Network diagram for the NTP server/client mode configuration



Configuration procedure

Perform the following configurations on Device B.

View the NTP status of Device B before synchronization.

```
<DeviceB> display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 60.0002 Hz
 Actual frequency: 60.0002 Hz
 Clock precision: 2^18
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900 (00000000.00000000)
```

Set Device A as the NTP server of Device B.

```
<DeviceB> system-view
[DeviceB] ntp-service unicast-server 1.0.1.11
```

(After the above configurations, Device B is synchronized to Device A.) View the NTP status of Device B.

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 60.0002 Hz
 Actual frequency: 60.0002 Hz
 Clock precision: 2^18
 Clock offset: 0.66 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 7 2006 (BF422AE4.05AEA86C)
```

The above output information indicates that Device B is synchronized to Device A, and the stratum level of its clock is 3, one level lower than that of Device A.

View the information about NTP sessions of Device B. (You can see that Device B establishes a connection with Device A.)

```
[DeviceB] display ntp-service sessions
     source        reference       stra reach poll  now offset  delay disper
**************************************************************************
```

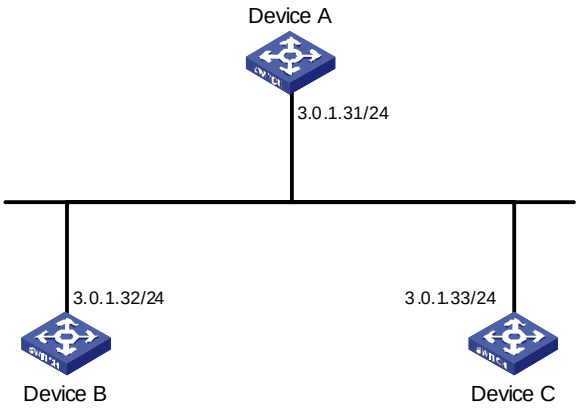
```
[12345]1.0.1.11    127.127.1.0     2    1    64    1    350.1    15.1    0.0
note:  1  source(master),2  source(peer),3  selected,4  candidate,5  configured  Total
associations :  1
```

Configuring NTP Symmetric Peer Mode

Network requirements

- As shown in Figure 1-7, the local clock of Device A is set as the NTP master clock, with the clock stratum level of 2.
- Device C (a WX3000 series device) uses Device A as the NTP server, and Device A works in server mode automatically.
- The local clock of Device B is set as the NTP master clock, with the clock stratum level of 1. Set Device C as the peer of Device B.

Figure 1-7 Network diagram for NTP peer mode configuration



Configuration procedure

1) Configure Device C.

Set Device A as the NTP server.

```
<DeviceC> system-view
[DeviceC] ntp-service unicast-server 3.0.1.31
```

2) Configure Device B (after the Device C is synchronized to Device A).

Enter system view.

```
<DeviceB> system-view
```

Set Device C as the peer of Device B.

```
[DeviceB] ntp-service unicast-peer 3.0.1.33
```

Device C and Device B are symmetric peers after the above configuration. Device B works in symmetric active mode, while Device C works in symmetric passive mode. Because the stratum level of the local clock of Device B is 1, and that of Device C is 3, the clock of Device C is synchronized to that of Device B.

View the status of Device C after the clock synchronization.

```
[DeviceC] display ntp-service status
 Clock status: synchronized
 Clock stratum: 2
```

```
Reference clock ID: 3.0.1.32
Nominal frequency: 60.0002 Hz
Actual frequency: 60.0002 Hz
Clock precision: 2^18
Clock offset: 0.66 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu Sep 7 2006 (BF422AE4.05AEA86C)
```

The output information indicates that the clock of Device C is synchronized to that of Device B and the stratum level of its local clock is 2, one level lower than Device B.

View the information about the NTP sessions of Device C (you can see that a connection is established between Device C and Device B).

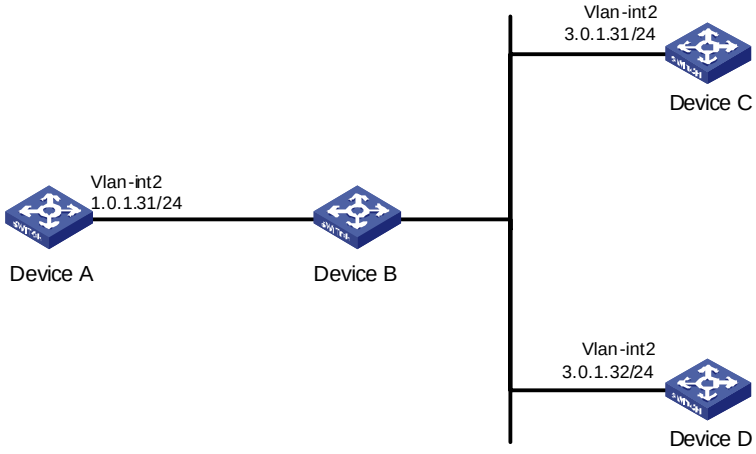
```
[DeviceC] display ntp-service sessions
     source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[1234]3.0.1.32    LOCL                1    95   64   42  -14.3   12.9    2.7
[25]3.0.1.31    127.127.1.0           2     1   64    1 4408.6   38.7    0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  2
```

Configuring NTP Broadcast Mode

Network requirements

- As shown in Figure 1-8, the local clock of Device C is set as the NTP master clock, with a stratum level of 2. Configure Device C to work in the NTP broadcast server mode and send NTP broadcast messages through Vlan-interface2.
- Device A and Device D are two WX3000 series devices. Configure Device A and Device D to work in the NTP broadcast client mode and listen to broadcast messages through their own Vlan-interface2.

Figure 1-8 Network diagram for the NTP broadcast mode configuration



Configuration procedure

1) Configure Device C.

Enter system view.

```
<DeviceC> system-view
```

Set Device C as the broadcast server, which sends broadcast messages through Vlan-interface2.

```
[DeviceC] interface Vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service broadcast-server
```

2) Configure Device A. (perform the same configuration on Device D)

Enter system view.

```
<DeviceA> system-view
```

Set Device A as a broadcast client.

```
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service broadcast-client
```

After the above configurations, Device A and Device D will listen to broadcast messages through their own Vlan-interface2, and Device C will send broadcast messages through Vlan-interface2. Because Device A and Device C do not share the same network segment, Device A cannot receive broadcast messages from Device C, while Device D is synchronized to Device C after receiving broadcast messages from Device C.

View the NTP status of Device D after the clock synchronization.

```
[DeviceD] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 60.0002 Hz
 Actual frequency: 60.0002 Hz
 Clock precision: 2^18
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 7 2006 (BF422AE4.05AEA86C)
```

The output information indicates that Device D is synchronized to Device C, with the clock stratum level of 3, one level lower than that of Device C.

View the information about the NTP sessions of Device D and you can see that a connection is established between Device D and Device C.

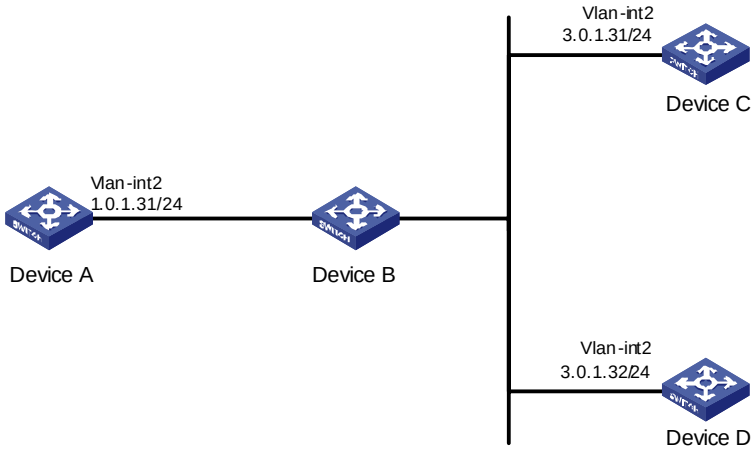
```
[DeviceD] display ntp-service sessions
    source          reference       stra reach poll  now offset   delay disper
**************************************************************************
[1234]3.0.1.31     127.127.1.0      2    1    64   377    26.1   199.53   9.7
note:  1  source(master),2  source(peer),3  selected,4  candidate,5  configured  Total
associations :  1
```

Configuring NTP Multicast Mode

Network requirements

- As shown in Figure 1-9, the local clock of Device C is set as the NTP master clock, with a clock stratum level of 2. Configure Device C to work in the NTP multicast server mode and advertise multicast NTP messages through Vlan-interface2.
- Device A and Device D are two WX3000 series devices. Configure Device A and Device D to work in the NTP multicast client mode and listen to multicast messages through their own Vlan-interface2.

Figure 1-9 Network diagram for NTP multicast mode configuration



Configuration procedure

1) Configure Device C.

Enter system view.

```
<DeviceC> system-view
```

Set Device C as a multicast server to send multicast messages through Vlan-interface2.

```
[DeviceC] interface Vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service multicast-server
```

2) Configure Device A (perform the same configuration on Device D).

Enter system view.

```
<DeviceA> system-view
```

Set Device A as a multicast client to listen to multicast messages through Vlan-interface2.

```
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service multicast-client
```

After the above configurations, Device A and Device D respectively listen to multicast messages through their own Vlan-interface2, and Device C advertises multicast messages through Vlan-interface2. Because Device A and Device C do not share the same network segment, Device A cannot receive multicast messages from Device C, while Device D is synchronized to Device C after receiving multicast messages from Device C.

View the NTP status of Device D after the clock synchronization.

```
[DeviceD] display ntp-service status
```

```
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 60.0002 Hz
Actual frequency: 60.0002 Hz
Clock precision: 2^18
Clock offset: 198.7425 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu Sep 7 2006 (BF422AE4.05AEA86C)
```

The output information indicates that Device D is synchronized to Device C, with a clock stratum level of 3, one stratum level lower than that Device C.

View the information about the NTP sessions of Device D (You can see that a connection is established between Device D and Device C).

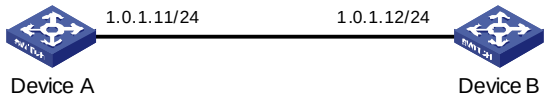
```
[DeviceD] display ntp-service sessions
   source        reference       stra reach poll  now offset  delay disper
**************************************************************************
[1234]3.0.1.31     127.127.1.0      2    1     64    377  26.1   199.53  9.7
note:  1  source(master),2  source(peer),3  selected,4  candidate,5  configured  Total
associations :  1
```

Configuring NTP Server/Client Mode with Authentication

Network requirements

- As shown in Figure 1-10, the local clock of Device A is set as the NTP master clock, with a clock stratum level of 2.
- Device B is a WX3000 series device and uses Device A as the NTP server. Device B is set to work in client mode, while Device A works in server mode automatically.
- The NTP authentication function is enabled on Device A and Device B.

Figure 1-10 Network diagram for NTP server/client mode with authentication configuration



Configuration procedure

1) Configure Device B.

Enter system view.

```
<DeviceB> system-view
```

Set Device A as the NTP server.

```
[DeviceB] ntp-service unicast-server 1.0.1.11
```

Enable the NTP authentication function.

```
[DeviceB] ntp-service authentication enable
```

Configure an MD5 authentication key, with the key ID being **42** and the key being **aNiceKey**.

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

Specify the key 42 as a trusted key.

```
[DeviceB] ntp-service reliable authentication-keyid 42
[DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

After the above configurations, Device B is ready to synchronize with Device A. Because the NTP authentication function is not enabled on Device A, the clock of Device B will fail to be synchronized to that of Device A.

2) To synchronize Device B, you need to perform the following configurations on Device A.

Enable the NTP authentication function.

```
[DeviceA] system-view
[DeviceA] ntp-service authentication enable
```

Configure an MD5 authentication key, with the key ID being **42** and the key being **aNiceKey**.

```
[DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

Specify the key 42 as a trusted key.

```
[DeviceA] ntp-service reliable authentication-keyid 42
```

(After the above configurations, the clock of Device B can be synchronized to that of Device A.) View the status of Device B after synchronization.

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 60.0002 Hz
 Actual frequency: 60.0002 Hz
 Clock precision: 2^18
 Clock offset: 0.66 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 7 2006 (BF422AE4.05AEA86C)
```

The output information indicates that the clock of Device B is synchronized to that of Device A, with a clock stratum level of 3, one stratum level lower than that Device A.

View the information about NTP sessions of Device B (You can see that a connection is established between Device B and Device A).

```
<DeviceB> display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************        [12345]
1.0.1.11    127.127.1.0        2   255   64    8    2.8   17.7    1.2
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

Table of Contents

1 SSH Configuration 1-1

SSH Overview 1-1

Introduction to SSH 1-1

Algorithm and Key 1-1

Asymmetric Key Algorithm 1-2

SSH Operating Process 1-2

Configuring the SSH Server 1-4

SSH Server Configuration Tasks 1-5

Configuring the Protocol Support for the User Interface 1-5

Generating/Destroying a RSA or DSA Key Pair 1-6

Exporting the RSA or DSA Public Key 1-7

Creating an SSH User and Specify an Authentication Type 1-7

Specifying a Service Type for an SSH User 1-8

Configuring SSH Management 1-8

Configuring the Client Public Key on the Server 1-9

Assigning a Public Key to an SSH User 1-11

Specifying a Source IP Address/Interface for the SSH Server 1-11

Configuring the SSH Client 1-12

SSH Client Configuration Tasks 1-12

Configuring the SSH Client Using an SSH Client Software 1-12

Configuring the SSH Client on an SSH2-Capable Device 1-19

Specifying a Source IP address/Interface for the SSH client 1-21

Displaying and Maintaining SSH Configuration 1-21

SSH Configuration Examples 1-22

When the Device Acts as the SSH Server and the Authentication Type is Password 1-22

When the Device Acts as an SSH Server and the Authentication Type is Publickey 1-24

When the Switch Acts as an SSH Client and the Authentication Type is Password 1-30

When the Device Acts as an SSH Client and the Authentication Type is Publickey 1-31

When the Device Acts as an SSH Client and First-time authentication is not Supported 1-33

1 SSH Configuration

Note

- The term switch used throughout this document refers to a switching device in a generic sense or the switching engine of a WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary

SSH Overview

Introduction to SSH

Secure Shell (SSH) is a protocol that provides secure remote login and other security services in insecure network environments. In an SSH connection, data are encrypted before being sent out and decrypted after they reach the destination. This prevents attacks such as plain text password interception. Besides, SSH also provides powerful user authentication functions that prevent attacks such as DNS and IP spoofing.

SSH adopts the client-server model. The device can be configured as an SSH client or an SSH server. In the former case, the device establishes a remote SSH connection to an SSH server. In the latter case, the device provides connections to multiple clients.

Furthermore, SSH can also provide data compression to increase transmission speed, take the place of Telnet or provide a secure “channel” for FTP.

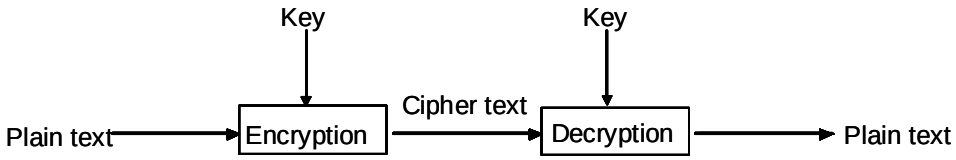
Caution

- Currently, the device that serves as an SSH server supports two SSH versions: SSH2 and SSH1, and the device that serves as an SSH client supports only SSH2.
- Unless otherwise noted, SSH refers to SSH2 throughout this document.

Algorithm and Key

Algorithm is a set of transformation rules for encryption and decryption. Information without being encrypted is known as plain text, while information that is encrypted is known as cipher text. Encryption and decryption are performed using a string of characters called a key, which controls the transformation between plain text and cipher text, for example, changing the plain text into cipher text or cipher text into plain text.

Figure 1-1 Encryption and decryption



Key-based algorithm is usually classified into symmetric key algorithm and asymmetric key algorithm.

Asymmetric Key Algorithm

Asymmetric key algorithm means that a key pair exists at both ends. The key pair consists of a private key and a public key. The public key is effective for both ends, while the private key is effective only for the local end. Normally you cannot use the private key through the public key.

Asymmetric key algorithm encrypts data using the public key and decrypts the data using the private key, thus ensuring data security.

You can also use the asymmetric key algorithm for data signature. For example, user 1 adds his signature to the data using the private key, and then sends the data to user 2. User 2 verifies the signature using the public key of user 1. If the signature is correct, this means that the data originates from user 1.

Both Revest-Shamir-Adleman Algorithm (RSA) and Digital Signature Algorithm (DSA) are asymmetric key algorithms. RSA is used for data encryption and signature, whereas DSA is used for adding signature.

Note

Currently, SSH supports both RSA and DSA.

SSH Operating Process

The session establishment between an SSH client and the SSH server involves the following five stages:

Table 1-1 Stages in establishing a session between the SSH client and server

Stages	Description
Version negotiation	SSH1 and SSH2 are supported. The two parties negotiate a version to use.
Key and algorithm negotiation	SSH supports multiple algorithms. The two parties negotiate an algorithm for communication.
Authentication	The SSH server authenticates the client in response to the client's authentication request.
Session request	This client sends a session request to the server.
Data exchange	The client and the server start to communicate with each other.

Version negotiation

- The server opens port 22 to listen to connection requests from clients.
- The client sends a TCP connection request to the server. After the TCP connection is established, the server sends the first packet to the client, which includes a version identification string in the format of “SSH-<primary protocol version number>.<secondary protocol version number>-<software version number>”. The primary and secondary protocol version numbers constitute the protocol version number, while the software version number is used for debugging.
- The client receives and resolves the packet. If the protocol version of the server is lower but supportable, the client uses the protocol version of the server; otherwise, the client uses its own protocol version.
- The client sends to the server a packet that contains the number of the protocol version it decides to use. The server compares the version carried in the packet with that of its own to determine whether it can cooperate with the client.
- If the negotiation is successful, the server and the client go on to the key and algorithm negotiation. If not, the server breaks the TCP connection.

Note

All the packets above are transferred in plain text.

Key negotiation

- The server and the client send algorithm negotiation packets to each other, which contain public key algorithm lists supported by the server and the client, encrypted algorithm list, message authentication code (MAC) algorithm list, and compressed algorithm list.
- The server and the client calculate the final algorithm according to the algorithm lists supported.
- The server and the client generate the session key and session ID based on the Diffie-Hellman (DH) exchange algorithm and the host key pair.
- Then, the server and the client get the same session key and use it for data encryption and decryption to secure data communication.

Authentication negotiation

The negotiation steps are as follows:

- The client sends an authentication request to the server. The authentication request contains username, authentication type, and authentication-related information. For example, if the authentication type is **password**, the content is the password.
- The server starts to authenticate the user. If authentication fails, the server sends an authentication failure message to the client, which contains the list of methods used for a new authentication process.
- The client selects an authentication type from the method list to perform authentication again.
- The above process repeats until the authentication succeeds, or the connection is torn down when the authentication times reach the upper limit.

SSH provides two authentication methods: password authentication and publickey authentication.

- In password authentication, the client encrypts the username and password, encapsulates them into a password authentication request, and sends the request to the server. Upon receiving the request, the server decrypts the username and password, compares them with those it maintains, and then informs the client of the authentication result.
- The publickey authentication method authenticates clients using digital signatures. Currently, the device supports two publickey algorithms to implement digital signatures: RSA and DSA. The client sends to the server a publickey authentication request containing its user name, public key and algorithm. The server verifies the public key. If the public key is invalid, the authentication fails; otherwise, the server generates a digital signature to authenticate the client, and then sends back a message to inform the success or failure of the authentication.

Session request

After passing authentication, the client sends a session request to the server, while the server listens to and processes the request from the client. If the client passes authentication, the server sends back to the client an SSH_SMSG_SUCCESS packet and goes on to the interactive session stage with the client. Otherwise, the server sends back to the client an SSH_SMSG_FAILURE packet, indicating that the processing fails or it cannot resolve the request. The client sends a session request to the server, which processes the request and establishes a session.

Data exchange

In this stage, the server and the client exchanges data in this way:

- The client encrypts and sends the command to be executed to the server.
- The server decrypts and executes the command, and then encrypts and sends the result to the client.
- The client decrypts and displays the result on the terminal.

Configuring the SSH Server

You must perform necessary configurations on the SSH server for SSH clients to access.

SSH Server Configuration Tasks

Complete the following tasks to configure SSH server:

Task		Remark
Configuring the SSH server	Configuring the Protocol Support for the User Interface	Required
	Generating/Destroying a RSA or DSA Key Pair	Required
	Exporting the RSA or DSA Public Key	Optional
	Creating an SSH User and Specify an Authentication Type	Required
	Specifying a Service Type for an SSH User	Optional
	Configuring SSH Management	Optional
	Configuring the Client Public Key on the Server	Required for **pubilckey** authentication; unnecessary for **password** authentication
	Assigning a Public Key to an SSH User	Required for **pubilckey** authentication; unnecessary for **password** authentication
	Specifying a Source IP Address/Interface for the SSH Server	Optional

Configuring the Protocol Support for the User Interface

You must configure the supported protocol(s) for SSH remote login. Note that the configuration does not take effect immediately, but will be effective for subsequent login requests.

Follow these steps to configure the protocol(s) that a user interface supports:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter the view of one or multiple user interfaces	**user-interface** [*type*] *first-number* [*last-number*]	—
Configure the authentication mode as scheme	**authentication-mode scheme** [**command-authorization**]	Required By default, the user interface authentication mode is password
Specify the supported protocol(s)	**protocol inbound** { **all** |**ssh** | **telnet** }	Optional By default, both Telnet and SSH are supported.

Caution

- If you have configured a user interface to support SSH protocol, you must configure AAA authentication for the user interface by using the **authentication-mode scheme** command to ensure successful login.
- On a user interface, if the **authentication-mode password** or **authentication-mode none** command has been executed, the **protocol inbound ssh** command is not available. Similarly, if the **protocol inbound ssh** command has been executed, the **authentication-mode password** and **authentication-mode none** commands are not available.

Generating/Destroying a RSA or DSA Key Pair

This configuration task lets you generate or destroy a key pair. You must generate an RSA or DSA key pair on the server for an SSH client to log in successfully. When generating a key pair, you will be prompted to enter the key length in bits, which is between 512 and 2048. In case a key pair already exists, the system will ask whether to replace the existing key pair.

Follow these steps to create or destroy a key pair:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Generate an RSA key pair	**rsa local-key-pair create**	Required Use either command By default, no RSA key pair is created.
	public-key local create rsa	
Destroy the RSA key pair	**rsa local-key-pair destroy**	Optional Use either command to destroy the configured RSA key pair.
	public-key local destroy rsa	
Generate a DSA key pair	**public-key local create dsa**	Required By default, no DSA key pair is created.
Destroy the DSA key pair	**public-key local destroy dsa**	Optional Use the command to destroy the configured DSA key pair.

Note

- After an RSA key pair is generated, you can execute the **display rsa local-key-pair public** or **display public-key local rsa public** command, which will display two public keys (the host public key and server public key) if the device works in SSH1.x-compatible mode, or only one public key (the host public key) if the device works in SSH2 mode.
- The command for generating a key pair can survive a reboot. You only need to configure it once.
- Some third-party software, for example, WinSCP, requires that the modulo of a public key be greater than or equal to 768. Therefore, a local key pair of more than 768 bits is recommended.

Exporting the RSA or DSA Public Key

You can display the generated RSA or DSA key pair on the screen in a specified format, or export it to a specified file for configuring the key at a remote end.

Follow these steps to export the RSA public key:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Display the RSA key on the screen in a specified format or export it to a specified file	**public-key local export rsa** { **openssh** | **ssh1** | **ssh2** } [*filnename*]	Required

Follow these steps to export the DSA public key:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Display the DSA key on the screen in a specified format or export it to a specified file	**public-key local export dsa** { **openssh** | **ssh2** } [*filnename*]	Required

Note

The DSA public key format can be SSH2 and OpenSSH, while the RSA public key format can be SSH1, SSH2 and OpenSSH.

Creating an SSH User and Specify an Authentication Type

This task is to create an SSH user and specify an authentication type for it. Specifying an authentication type for a new user is a must to get the user login.

Follow these steps to configure an SSH user and specify an authentication type for it:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify the default authentication type for all SSH users	**ssh authentication-type default** { **all** | **password** | **password-publickey** | **publickey** | **rsa** }	Use either command. By default, no SSH user is created and no authentication type is specified. Note that: If both commands are used and different authentication types are specified, the authentication type specified with the **ssh user authentication-type** command takes precedence.
	ssh user *username*	
Create an SSH user, and specify an authentication type for it	**ssh user** *username* **authentication-type** { **all** | **password** | **password-publickey** | **publickey** | **rsa** }	

Caution

- For **password** authentication type, the *username* argument must be consistent with the valid user name defined in AAA; for publickey authentication, the *username* argument is the SSH local user name, so that there is no need to configure a local user in AAA.
- If the default authentication type for SSH users is **password** and local AAA authentication is adopted, you need not use the **ssh user** command to create an SSH user. Instead, you can use the **local-user** command to create a user name and its password and then set the service type of the user to SSH.
- If the default authentication type for SSH users is password and remote authentication (RADIUS authentication, for example) is adopted, you need not use the **ssh user** command to create an SSH user, because it is created on the remote server. And the user can use its username and password configured on the remote server to access the network.
- Both publickey and rsa indicate public key authentication. They are implemented with the same method.
- Under the **publickey** authentication mode, the level of commands available to a logged-in SSH user can be configured using the **user privilege level** command on the server, and all the users with this authentication mode will enjoy this level.
- Under the **password** authentication mode, the level of commands available to a logged-in SSH user is determined by AAA, and different users with this authentication mode may enjoy different levels.

Specifying a Service Type for an SSH User

Follow these steps to specify the service type of an SSH user:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify a service type for an SSH user	**ssh user** *username* **service-type** { **stelnet** | **sftp** | **all** }	Required **stelnet** by default

Caution

If the **ssh user service-type** command is executed with a username that does not exist, the system will automatically create the SSH user. However, the user cannot log in unless you specify an authentication type for it.

Configuring SSH Management

The SSH server provides a number of management functions that prevent illegal operations such as malicious password guess, to further guarantee the security of SSH connections.

Follow these steps to configure SSH management:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set SSH authentication timeout time	**ssh server timeout** *seconds*	Optional By default, the timeout time is 60 seconds.
Set SSH authentication retry times	**ssh server authentication-retries** *times*	Optional By default, the number of retry times is 3.
Set RSA server key update interval	**ssh server rekey-interval** *hours*	Optional By default, the system does not update RSA server keys.
Configure SSH server to be compatible with SSH1.x clients	**ssh server compatible-ssh1x enable**	Optional By default, SSH server is compatible with SSH1.x clients.
Configure a login header	**header shell** *text*	Optional By default, no login header is configured.

Caution

- You can configure a login header only when the service type is **stelnet**. For configuration of service types, see Specifying a Service Type for an SSH User.
- For details of the **header** command, see the corresponding section in *Login Command*.

Configuring the Client Public Key on the Server

Note

This configuration is not necessary if the **password** authentication mode is configured for SSH users.

With the **publickey** authentication mode configured for an SSH client, you must configure the client's RSA or DSA host public key(s) on the server for authentication.

You can manually configure the public key or import it from a public key file. In the former case, you can manually copy the client's public key to the server. In the latter case, the system automatically converts the format of the public key generated by the client to complete the configuration on the server, but the client's public key should be transferred from the client to the server beforehand through FTP/TFTP.

Follow these steps to configure the client's public key manually:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter public key view	**public-key peer** *keyname*	Required

To do…	Use the command…	Remarks
Enter public key edit view	**public-key-code begin**	—
Configure a public key for the client	Enter the content of the public key	When you input the key data, spaces are allowed between the characters you input (because the system can remove the spaces automatically); you can also press <Enter> to continue your input at the next line. But the key you input should be a hexadecimal digit string coded in the public key format.
Return to public key view from public key edit view	**public-key-code end**	—
Exit public key view and return to system view	**peer-public-key end**	—

Follow these steps to import the RSA public key from a public key file:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Import the public key from a public key file	**public-key peer** *keyname* **import sshkey** *filename*	Required

You can also use the following commands to configure the client's RSA public key on the server.

Follow these steps to configure the client RSA public key manually:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter public key view	**rsa peer-public-key** *keyname*	Required
Enter public key edit view	**public-key-code begin**	—
Configure the client RSA public key	Enter the content of the RSA public key	The content must be a hexadecimal string that is generated randomly by the SSH-supported client software and coded compliant to PKCS. Spaces and carriage returns are allowed between characters.
Return from public key code view to public key view	**public-key-code end**	— When you exit public key code view, the system automatically saves the public key.
Return from public key view to system view	**peer-public-key end**	—

Follow these steps to import the RSA public key from a public key file:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Import the RSA public key from a public key file	**rsa peer-public-key** *keyname* **import sshkey** *filename*	Required

Note

The result of the **display rsa local-key-pair public** command or the public key converted with the SSHKEY tool contains no information such as the authentication type, so they cannot be directly used as parameters in the **public-key peer** command. For the same reason, neither can the result of the **display public-key local rsa public** command be used in the **rsa peer-public-key** command directly.

Assigning a Public Key to an SSH User

Caution

This configuration task is unnecessary if the SSH user's authentication mode is **password**.

For the **publickey** authentication mode, you must specify the client's public key on the server for authentication.

Follow these steps to assign a public key for an SSH user:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Assign a public key to an SSH user	**ssh user** *username* **assign** { **publickey** | **rsa-key** } *keyname*	Required If you issue this command multiple times, the last command overrides the previous ones.

Note

Both the keywords **publickey** and **rsa-key** represent the public key, and have the same implementation.

Specifying a Source IP Address/Interface for the SSH Server

This configuration task allows you to specify a source IP address or interface for the SSH server, which is used by clients as the destination.

Follow these steps to specify a source IP address/interface for the SSH server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify a source IP address for the SSH server	**ssh-server source-ip** *ip-address*	Required By default, the system determines the IP address for clients to access.
Specify a source interface for the SSH server	**ssh-server source-interface** *interface-type interface-number*	Required By default, the system determines the IP address for clients to access.

Configuring the SSH Client

An SSH client software or SSH2-capable device can serve as an SSH client to access the SSH server.

SSH Client Configuration Tasks

Complete the following tasks to configure SSH client:

Task		Remarks
Configuring the SSH client	Using an SSH client software	Use either approach
	On an SSH2-capable device	

Configuring the SSH Client Using an SSH Client Software

A variety of SSH client software are available, such as PuTTY and OpenSSH. For an SSH client to establish a connection with an SSH server, use the following commands:

Complete the following tasks to configure SSH client using a client software:

Task	Remarks
Generate a client key	Required for **publickey** authentication; unnecessary for **password** authentication
Specify the IP address of the Server	Required
Select a protocol for remote connection	Required
Select an SSH version	Required
Open an SSH connection with publickey authentication	Required for **publickey** authentication; unnecessary for **password** authentication
Open an SSH connection with password authentication	Required for **publickey** authentication; unnecessary for **password** authentication

Note

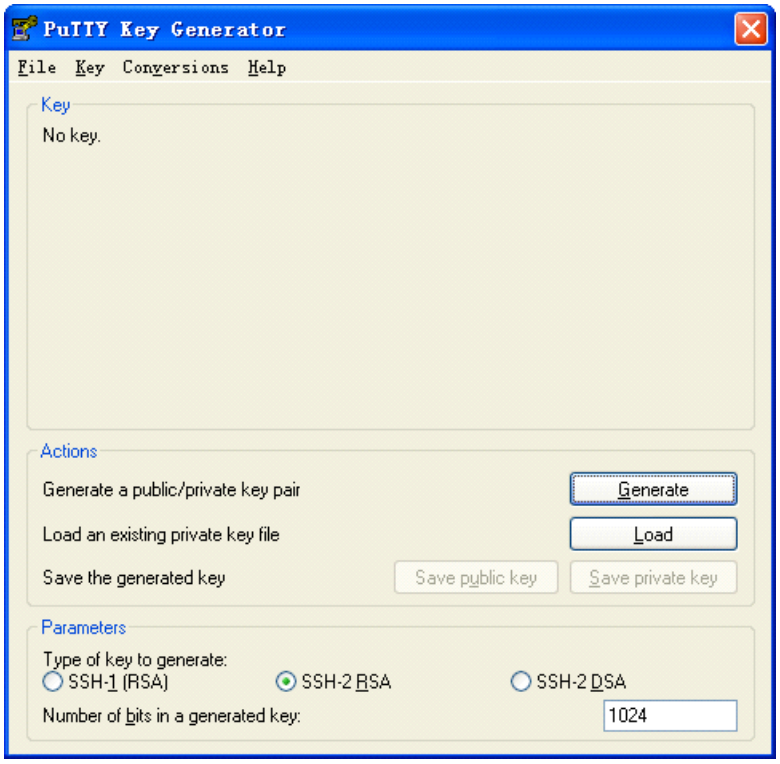
- Selecting the protocol for remote connection as SSH. Usually, a client can use a variety of remote connection protocols, such as Telnet, Rlogin, and SSH. To establish an SSH connection, you must select SSH
- Selecting the SSH version. Since the device supports SSH Server 2.0 now, select 2.0 or lower for the client.
- Specifying the private key file. On the server, if public key authentication is enabled for an SSH user and a public key is set for the user, the private key file corresponding to the public key must be specified on the client. RSA key pairs and DSA key pairs are generated by a tool of the client software.

The following takes the client software of PuTTY, PuTTYGen and SSHKEY as examples to illustrate how to configure the SSH client:

Generate a client key

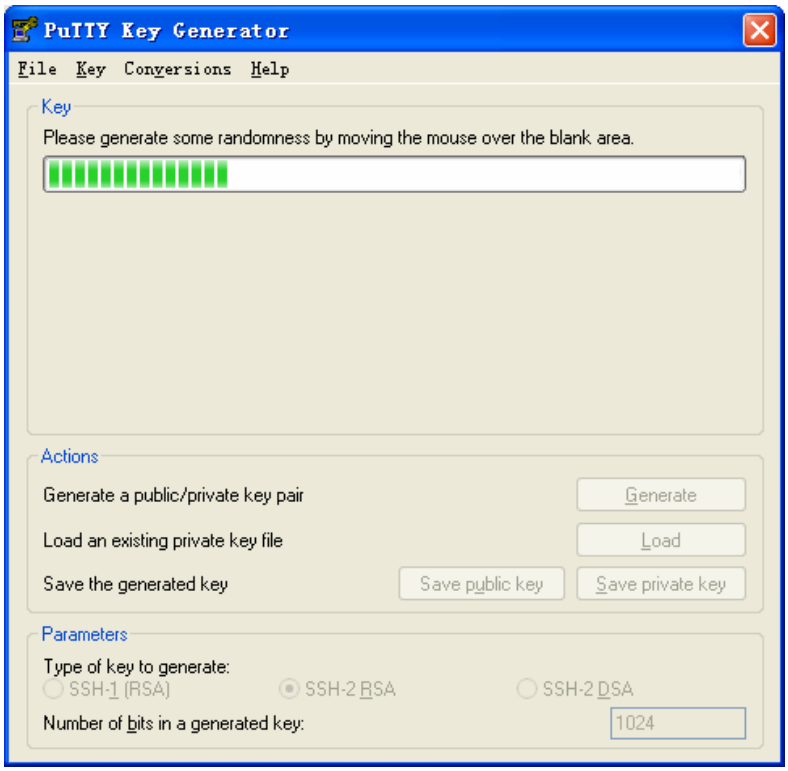
To generate a client key, run PuTTYGen.exe, and select from the **Parameters** area the type of key you want to generate, either SSH-2 RSA or SSH-2 DSA, then click **Generate.**

Figure 1-2 Generate a client key (1)



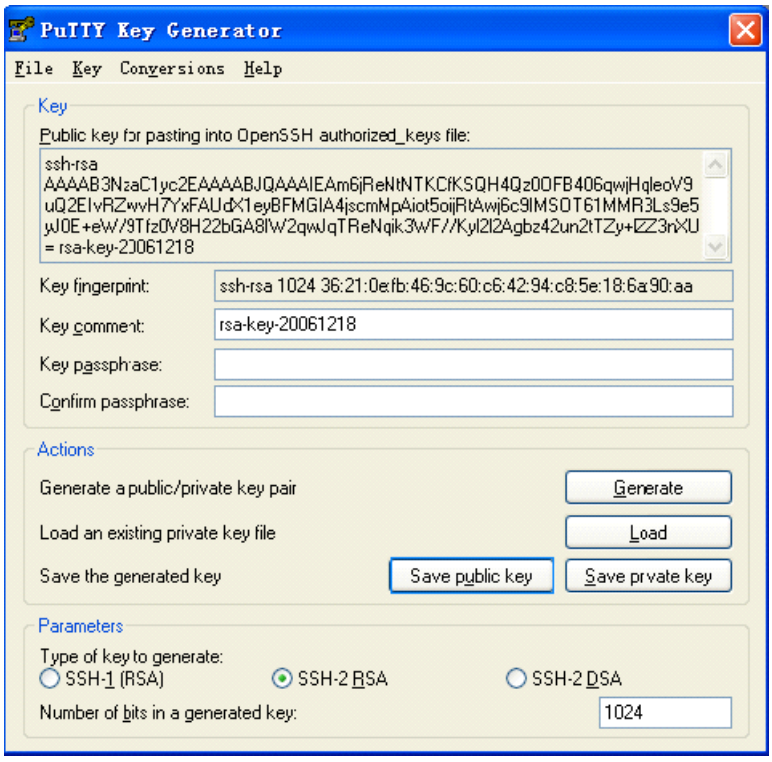
Note that while generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar in the blue box of shown in Figure 1-3. Otherwise, the process bar stops moving and the key pair generating process is stopped.

Figure 1-3 Generate the client keys (2)



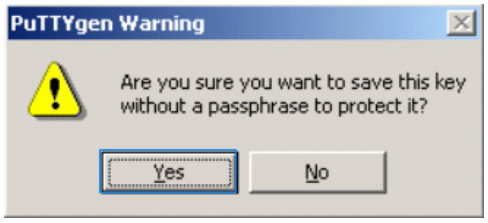
After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key (**public** in this case) to save the public key.

Figure 1-4 Generate the client keys (3)



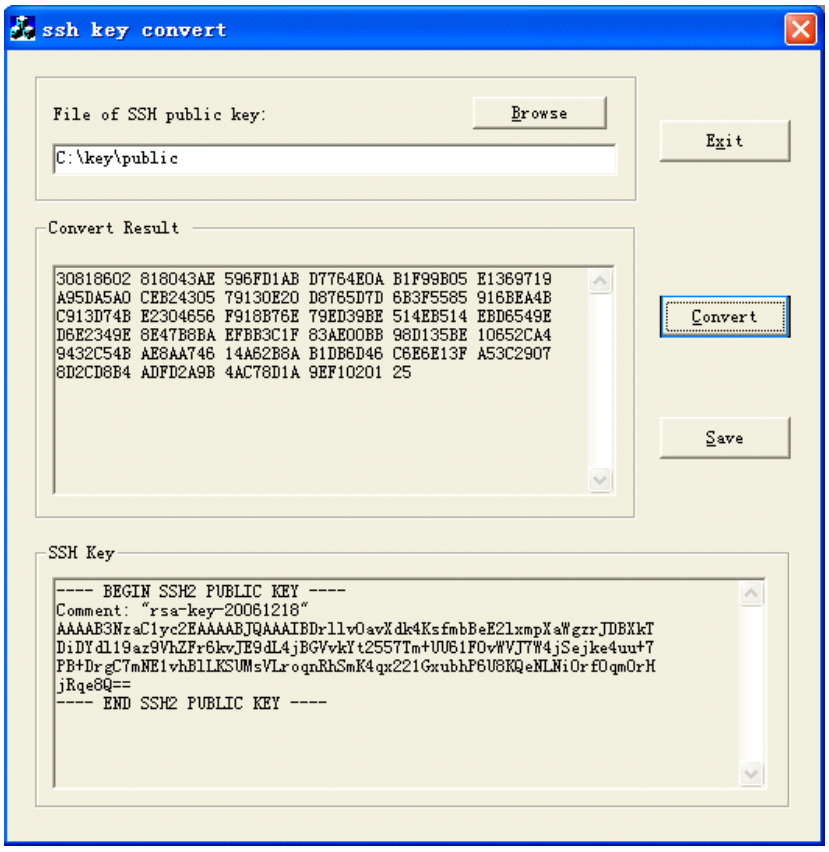
Likewise, to save the private key, click **Save private key**. A warning window pops up to prompt you whether to save the private key without any precaution. Click **Yes** and enter the name of the file for saving the private key (“private” in this case) to save the private key.

Figure 1-5 Generate the client keys (4)



To generate RSA public key in PKCS format, run SSHKEY.exe, click **Browse** and select the public key file, and then click **Convert**.

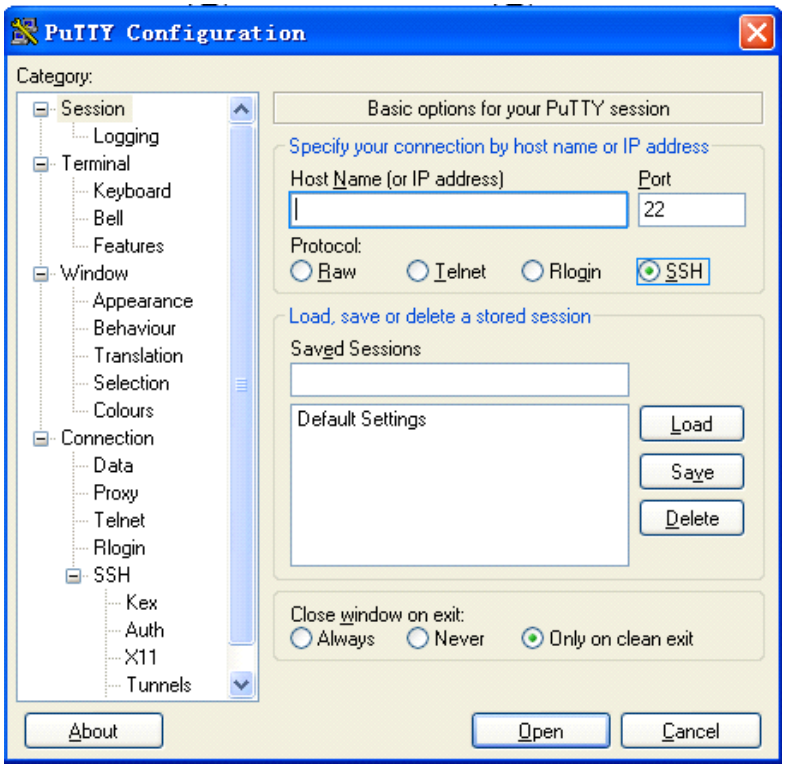
Figure 1-6 Generate the client keys (5)



Specify the IP address of the Server

Launch PuTTY.exe. The following window appears.

Figure 1-7 SSH client configuration interface 1



In the **Host Name (or IP address)** text box, enter the IP address of the server. Note that there must be a route available between the IP address of the server and the client.

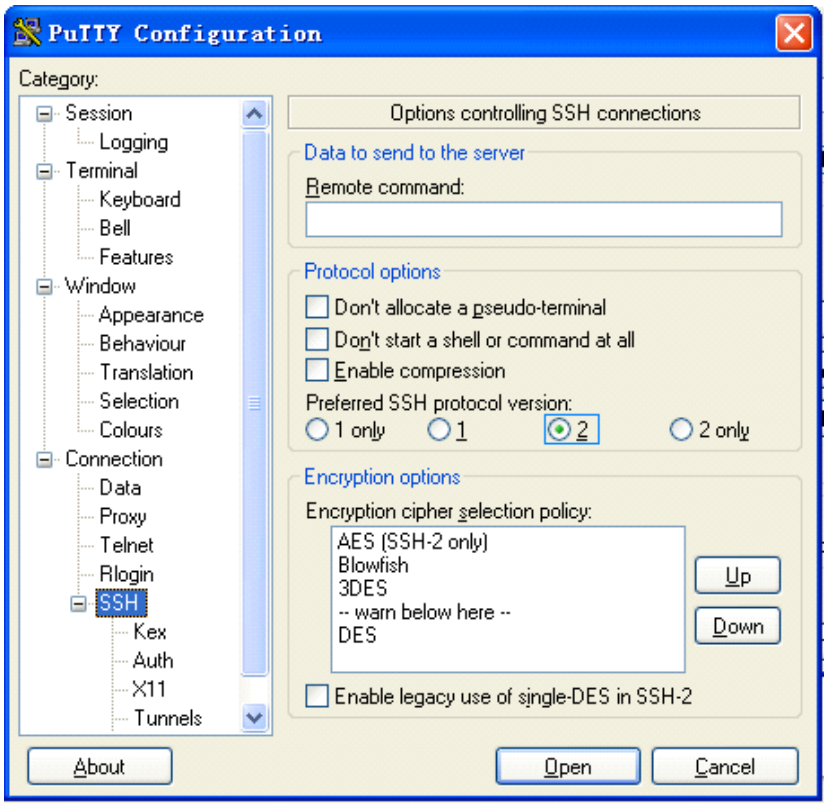
Select a protocol for remote connection

As shown in Figure 1-7, select **SSH** under **Protocol**.

Select an SSH version

From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 1-8 appears.

Figure 1-8 SSH client configuration interface 2



Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

Note

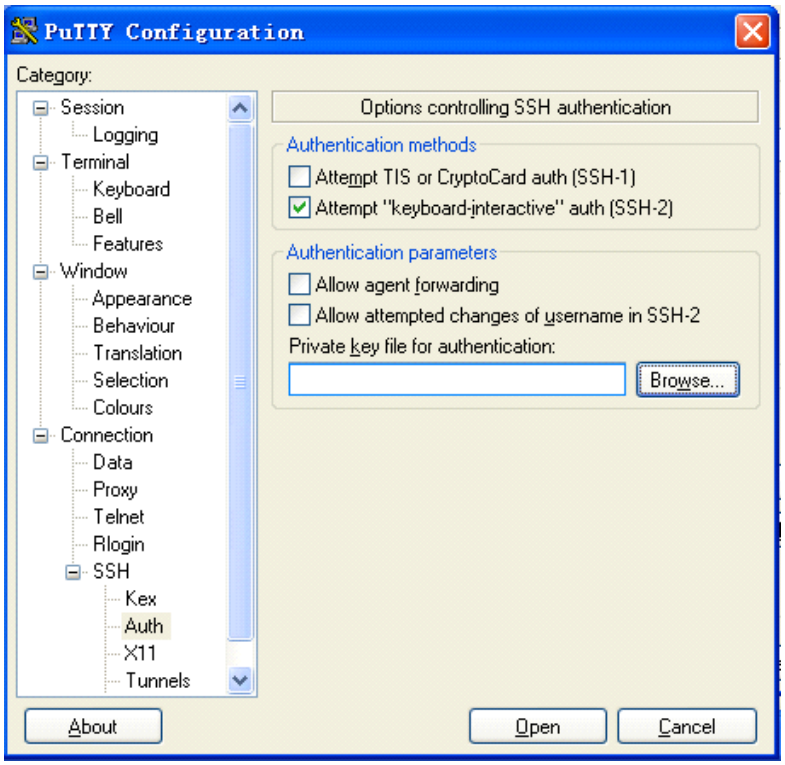
Some SSH client software, for example, Tectia client software, supports the DES algorithm only when the ssh1 version is selected. The PuTTY client software supports DES algorithm negotiation ssh2.

Open an SSH connection with publickey authentication

If a user needs to be authenticated with a public key, the corresponding private key file must be specified. A private key file is not required for password-only authentication.

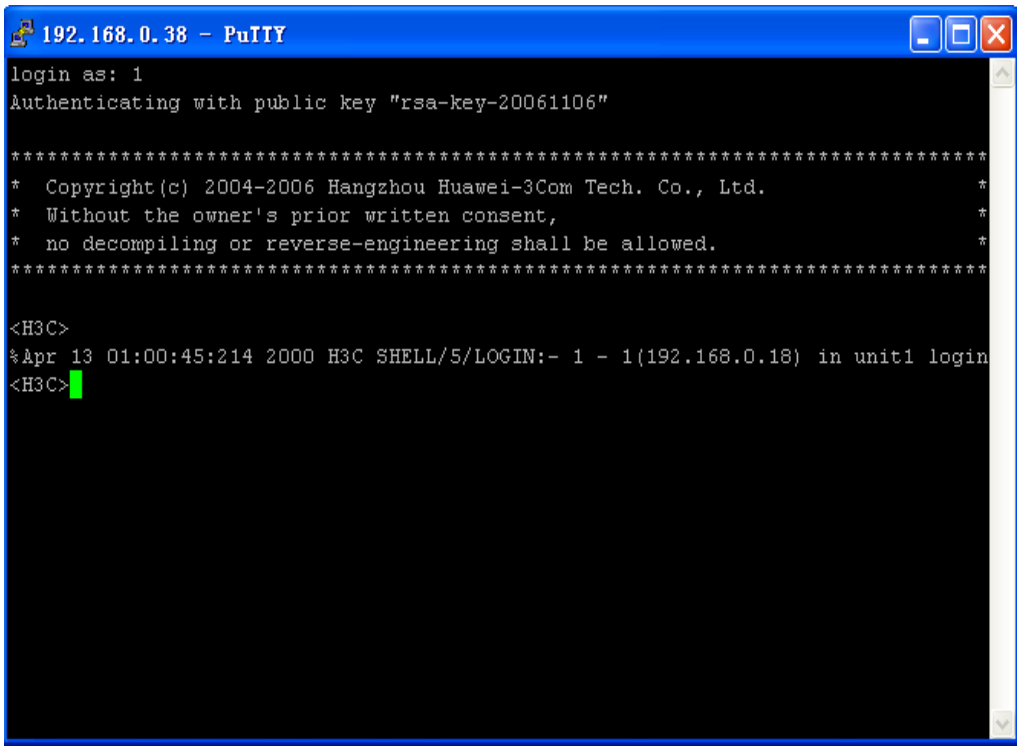
From the category on the left of the window, select **Connection/SSH/Auth**. The following window appears.

Figure 1-9 SSH client configuration interface 3



Click **Browse…** to bring up the file selection window, navigate to the private key file and click **Open** to enter the following SSH client interface. If the connection is normal, a user will be prompted for a username. Once passing the authentication, the user can log onto the server.

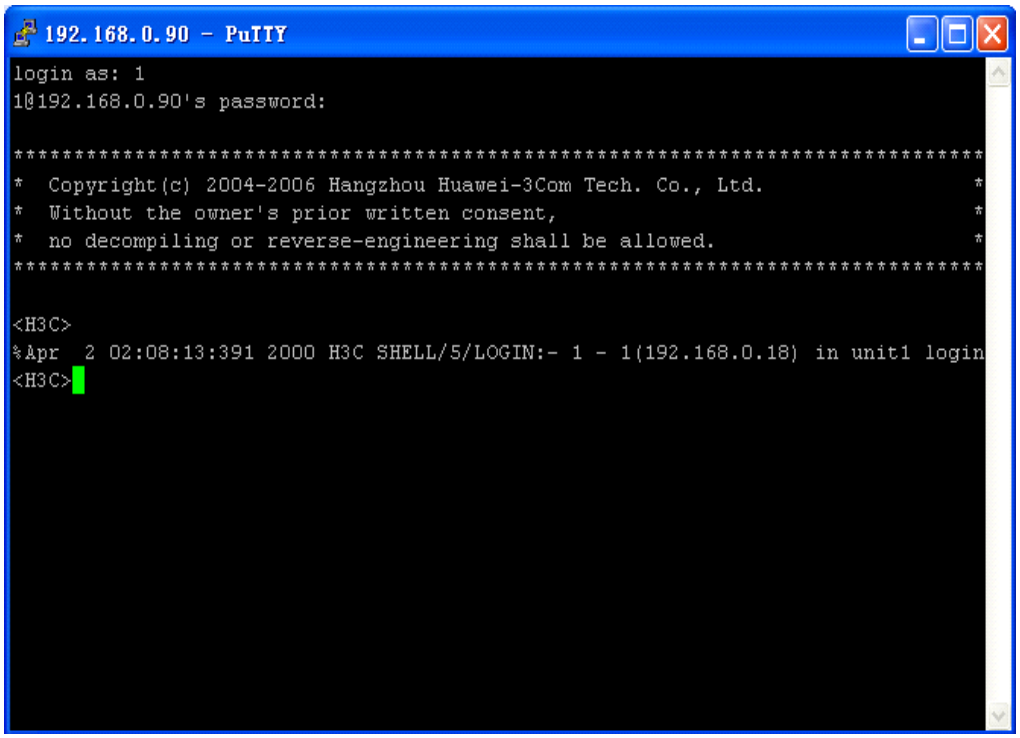
Figure 1-10 SSH client interface (1)



Open an SSH connection with password authentication

From the window shown in Figure 1-9, click Open. The following SSH client interface appears. If the connection is normal, you will be prompted to enter the username and password, as shown in Figure 1-11.

Figure 1-11 SSH client interface (2)



Enter the username and password to establish an SSH connection.

To log out, enter the **quit** command.

Configuring the SSH Client on an SSH2-Capable Device

Complete the following tasks to configure SSH client on an SSH2-capable device:

Task	Remarks
Configure whether first-time authentication is supported	Optional
Establish the connection between the SSH client and server	Required

Configure whether first-time authentication is supported

When the device connects to the SSH server as an SSH client, you can configure whether the device supports first-time authentication.

- First-time authentication means that when the SSH client accesses the server for the first time and is not configured with the server host public key, the user can continue accessing the server, and will save the host public key on the client for use in subsequent authentications.
- When first-time authentication is not supported, a client, if not configured with the server host public key, will be denied of access to the server. To access the server, a user must configure in advance the server host public key locally and specify the public key name for authentication.

Follow these steps to enable the device to support first-time authentication:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the device to support first-time authentication	**ssh client first-time enable**	Optional By default, the client is enabled to run initial authentication.

Follow these steps to disable first-time authentication support:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Disable first-time authentication support	**undo ssh client first-time**	Required By default, the client is enabled to run first-time authentication.
Configure server public key	Refer to Configuring the Client Public Key on the Server	Required The method of configuring server public key on the client is similar to that of configuring client public key on the server.
Specify the host key name of the server	**ssh client** { *server-ip* | *server-name* } **assign** { **publickey** | **rsa-key** } *keyname*	Required

Establish the connection between the SSH client and server

The client's method of establishing an SSH connection to the SSH server varies with authentication types. See the table below for details.

Follow these steps to establish an SSH connection:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Start the client to establish a connection with an SSH server	**ssh2** { *host-ip* | *host-name* } [*port-num*] [**identity-key** { **dsa** | **rsa** } | **prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128** } | **prefer_stoc_cipher** { **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *	Required In this command, you can also specify the preferred key exchange algorithm, encryption algorithms and HMAC algorithms between the server and client. HMAC: Hash-based message authentication code Note that: The **identity-key** keyword is unnecessary in password authentication and optional in public key authentication.

Note

When logging into the SSH server using public key authentication, an SSH client needs to read the local private key for authentication. As two algorithms (RSA or DSA) are available, the **identity-key** keyword must be used to specify one algorithm in order to get the correct private key.

Specifying a Source IP address/Interface for the SSH client

This configuration task allows you to specify a source IP address or interface for the client to access the SSH server, improving service manageability.

Follow these steps to specify a source IP address/interface for the SSH client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify a source IP address for the SSH client.	**ssh2 source-ip** *ip-address*	Required By default, the system determines a source IP address.
Specify a source interface for the SSH client	**ssh2 source-interface** *interface-type interface-number*	Required By default, the system determines a source IP address.

Displaying and Maintaining SSH Configuration

To do…	Use the command…	Remarks
Display host and server public keys	**display rsa local-key-pair public**	Available in any view
Display client RSA public key(s)	**display rsa peer-public-key** [**brief** | **name** *keyname*]	
Display local public key(s)	**display public-key local** { **dsa** | **rsa** } **public**	
Display remote public key(s)	**display public-key peer** [**brief** | **name** *pubkey-name*]	
Display SSH status and session information	**display ssh server** { **session** | **status** }	
Display SSH user information	**display ssh user-information** [*username*]	
Display the current source IP address or the IP address of the source interface specified for the SSH server.	**display ssh-server source-ip**	
Display the current source IP address specified for the SSH Client.	**display ssh2 source-ip**	
Display the mappings between host public keys and SSH servers saved on a client	**display ssh server-info**	

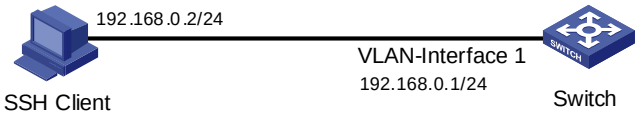
SSH Configuration Examples

When the Device Acts as the SSH Server and the Authentication Type is Password

Network requirements

As shown in Figure 1-12, establish an SSH connection between the host (SSH Client) and the device (SSH Server) for secure data exchange. The host runs SSH2.0 client software. Password authentication is required.

Figure 1-12 Network diagram of SSH server configuration using password authentication



Configuration procedure

- Configure the SSH server

Create a VLAN interface on the device and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<device> system-view
[device] interface vlan-interface 1
[device-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[device-Vlan-interface1] quit
```

Generate RSA and DSA key pairs.

```
[device] public-key local create rsa
[device] public-key local create dsa
```

Set the authentication mode for the user interfaces to AAA.

```
[device] user-interface vty 0 4
[device-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[device-ui-vty0-4] protocol inbound ssh
[device-ui-vty0-4] quit
```

Create local client “client001”, and set the authentication password to “abc”, protocol type to SSH, and command privilege level to 3 for the client.

```
[device] local-user client001
[device-luser-client001] password simple abc
[device-luser-client001] service-type ssh level 3
[device-luser-client001] quit
```

Specify the authentication method of user client001 as password.

```
[device] ssh user client001 authentication-type password
```

- Configure the SSH client

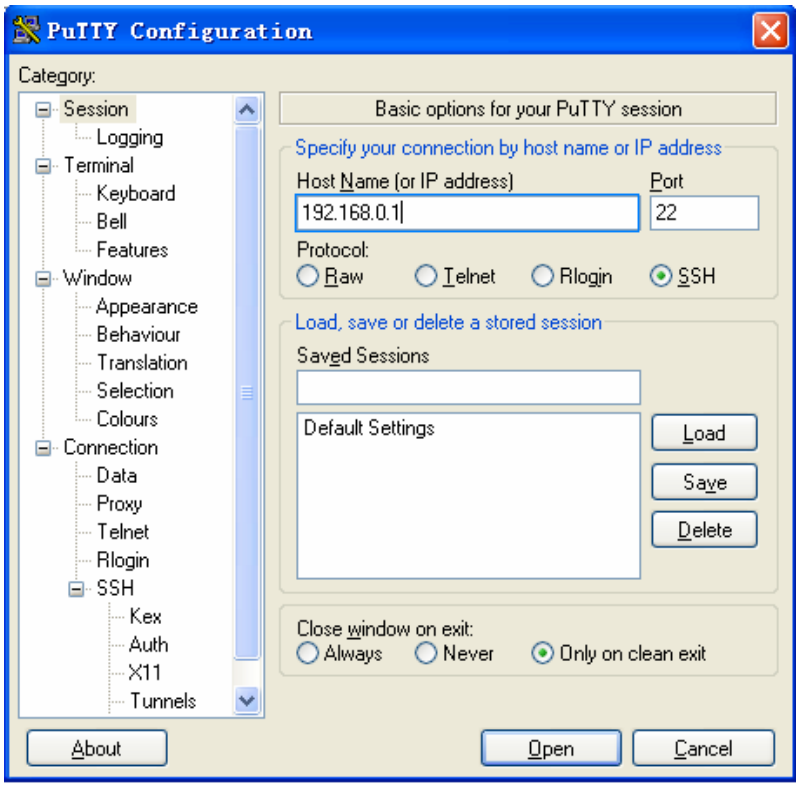
Configure an IP address (192.168.0.2 in this case) for the SSH client. This IP address and that of the VLAN interface on the device must be in the same network segment.

Configure the SSH client software to establish a connection to the SSH server.

Take SSH client software “Putty” (version 0.58) as an example:

1) Run PuTTY.exe to enter the following configuration interface.

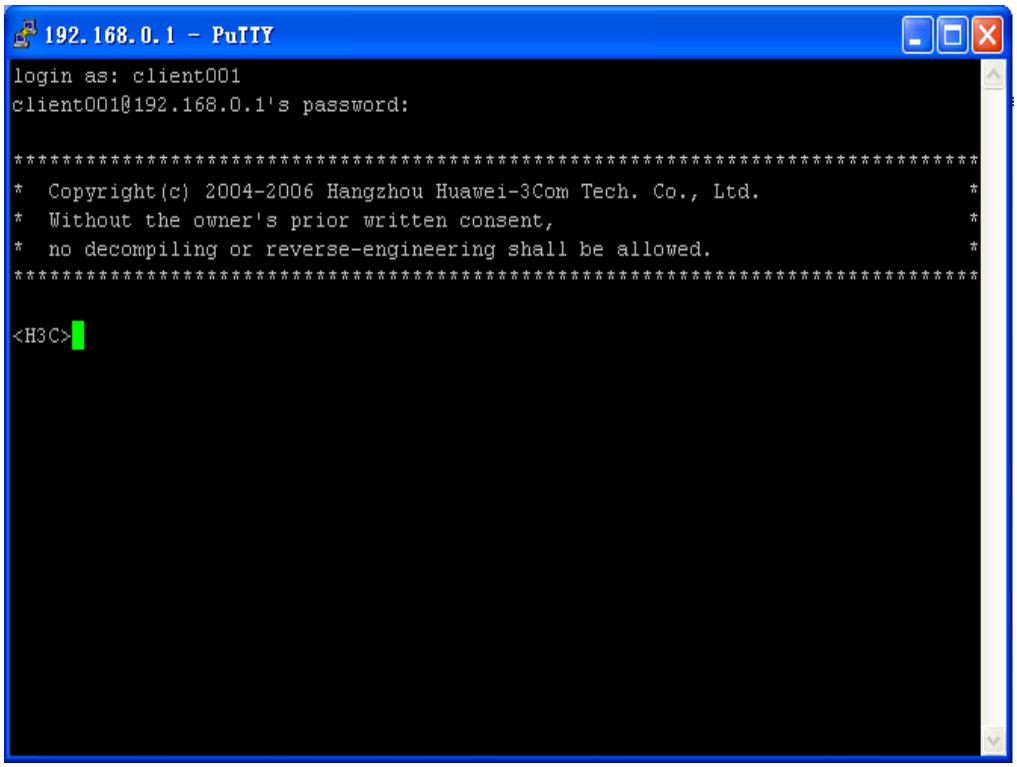
Figure 1-13 SSH client configuration interface



In the **Host Name (or IP address)** text box, enter the IP address of the SSH server.

2) As shown in Figure 1-13, click **Open** to enter the following interface. If the connection is normal, you will be prompted to enter the user name “client001” and password “abc”. Once authentication succeeds, you will log onto the server.

Figure 1-14 SSH client interface

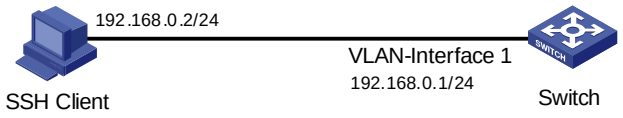


When the Device Acts as an SSH Server and the Authentication Type is Publickey

Network requirements

As shown in Figure 1-15, establish an SSH connection between the host (SSH client) and the device (SSH Server) for secure data exchange. The host runs SSH2.0 client software. Publickey authentication is required.

Figure 1-15 Network diagram of SSH server configuration



Configuration procedure

Note

Under the **publickey** authentication mode, either the RSA or DSA public key can be generated for the server to authenticate the client. Here takes the RSA public key as an example.

- Configure the SSH server

Create a VLAN interface on the device and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<device> system-view
[device] interface vlan-interface 1
[device-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[device-Vlan-interface1] quit
```

Generate RSA and DSA key pairs.

```
[device] public-key local create rsa
[device] public-key local create dsa
```

Set the authentication mode for the user interfaces to AAA.

```
[device] user-interface vty 0 4
[device-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[device-ui-vty0-4] protocol inbound ssh
```

Set the client's command privilege level to 3

```
[device-ui-vty0-4] user privilege level 3
[device-ui-vty0-4] quit
```

Configure the authentication type of the SSH client named client 001 as publickey.

```
[device] ssh user client001 authentication-type publickey
```



Note

Before performing the following steps, you must generate an RSA public key pair (using the client software) on the client, save the key pair in a file named public, and then upload the file to the SSH server through FTP or TFTP. For details, refer to *Configuring the SSH Client*.

Import the client's public key named "Switch001" from file "public".

```
[device] public-key peer Switch001 import sshkey public
```

Assign the public key "Switch001" to client "client001".

```
[device] ssh user client001 assign rsa-key Switch001
```

- Configure the SSH client

Generate an RSA key pair, taking PuTTYGen as an example.

Run PuTTYGen.exe, choose **SSH2(RSA)** and click **Generate**.

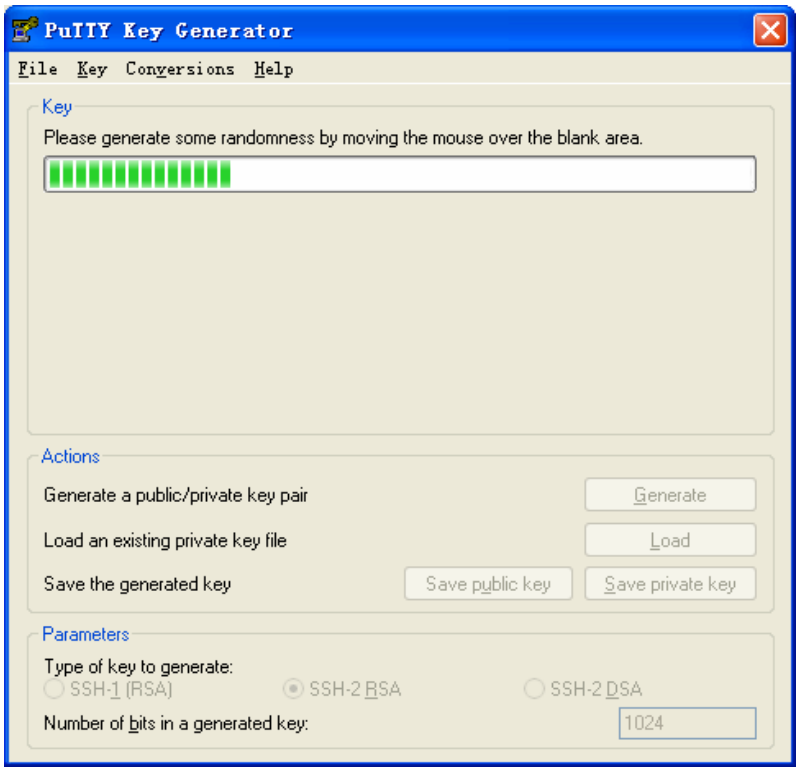
Figure 1-16 Generate a client key pair (1)



Note

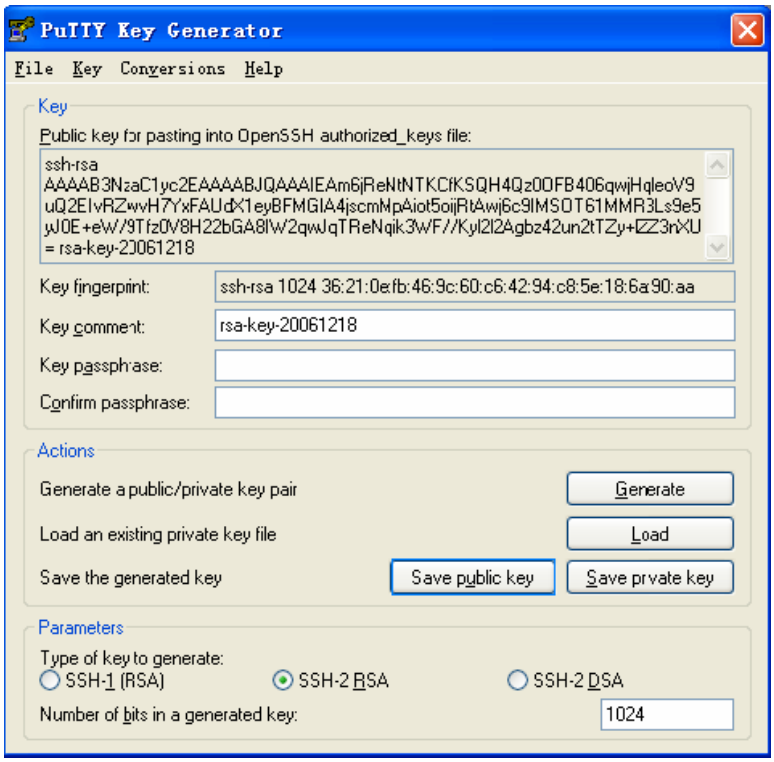
While generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar shown in Figure 1-17. Otherwise, the process bar stops moving and the key pair generating process is stopped.

Figure 1-17 Generate a client key pair (2)



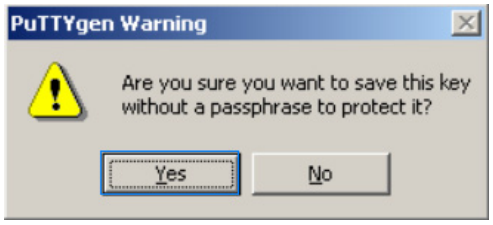
After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key (“public” in this case).

Figure 1-18 Generate a client key pair (3)



Likewise, to save the private key, click **Save private key**. A warning window pops up to prompt you whether to save the private key without any protection. Click **Yes** and enter the name of the file for saving the private key (“private” in this case).

Figure 1-19 Generate a client key pair (4)



Note

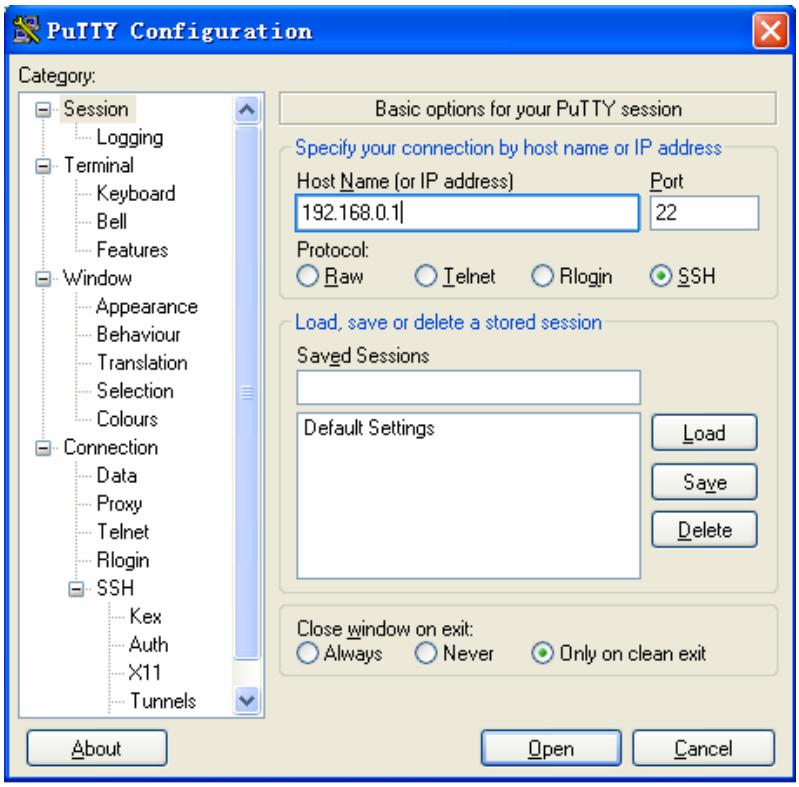
After a public key pair is generated, you need to upload the pubic key file to the server through FTP or TFTP, and complete the server end configuration before you continue to configure the client.

Establish a connection with the SSH server

The following takes the SSH client software Putty (version 0.58) as an example.

1) Launch PuTTY.exe to enter the following interface.

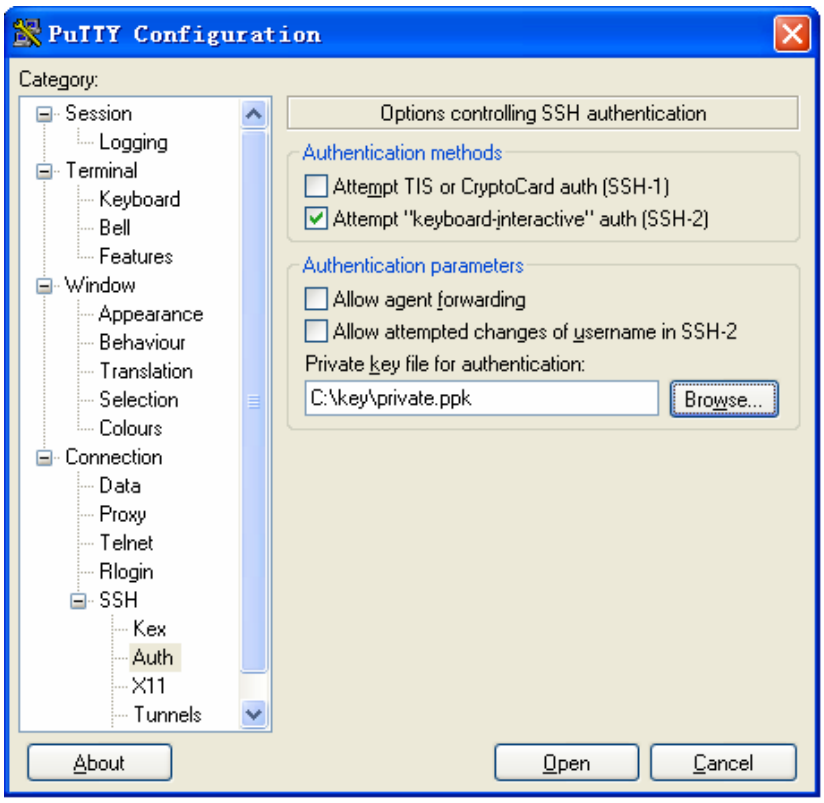
Figure 1-20 SSH client configuration interface 1



In the **Host Name (or IP address)** text box, enter the IP address of the server.

2) Select **Connection/SSH/Auth**. The following window appears.

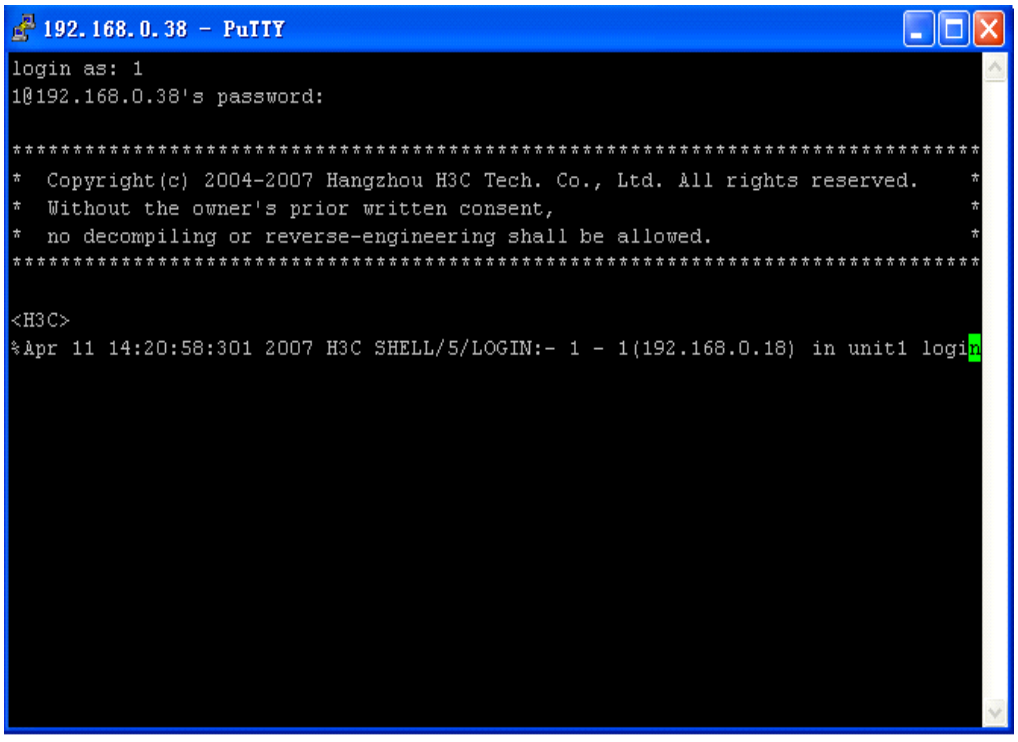
Figure 1-21 SSH client configuration interface (2)



Click **Browse…** to bring up the file selection window, navigate to the private key file and click **OK**.

3) From the window shown in Figure 1-21, click **Open**. The following SSH client interface appears. If the connection is normal, you will be prompted to enter the username and password, as shown in Figure 1-22.

Figure 1-22 SSH client interface

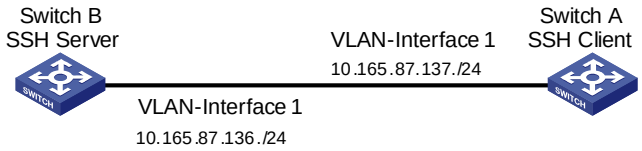


When the Switch Acts as an SSH Client and the Authentication Type is Password

Network requirements

As shown in Figure 1-23, establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name for login is client001 and the SSH server's IP address is 10.165.87.136. Password authentication is required.

Figure 1-23 Network diagram of SSH client configuration when using password authentication



Configuration procedure

- Configure Switch B

Create a VLAN interface on the device and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<device> system-view
[device] interface vlan-interface 1
[device-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[device-Vlan-interface1] quit
```

Generate RSA and DSA key pairs.

```
[device] public-key local create rsa
[device] public-key local create dsa
```

Set the authentication mode for the user interfaces to AAA.

```
[device] user-interface vty 0 4
[device-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[device-ui-vty0-4] protocol inbound ssh
[device-ui-vty0-4] quit
```

Create local user "client001", and set the authentication password to abc, the login protocol to SSH, and user command privilege level to 3.

```
[device] local-user client001
[device-luser-client001] password simple abc
[device-luser-client001] service-type ssh level 3
[device-luser-client001] quit
```

Configure the authentication type of user client001 as password.

```
[device] ssh user client001 authentication-type password
```

- Configure Switch A

Create a VLAN interface on the device and assign an IP address, which serves as the SSH client's address in an SSH connection.

```
<device> system-view
[device] interface vlan-interface 1
```

```
[device-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[device-Vlan-interface1] quit
```

Establish a connection to the server 10.165.87.136.

```
[device] ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):n
Enter password:

*****************************************************************************
*  Copyright(c) 2004-2009 3Com Corp. and its licensors. All rights reserved.   *
*  Without the owner's prior written consent,                                 *
*  no decompiling or reverse-engineering shall be allowed.                    *
*****************************************************************************

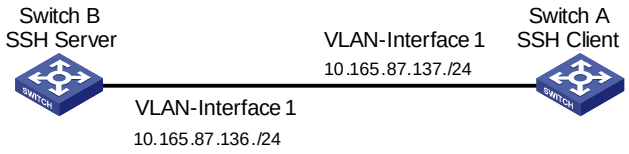
<device>
```

When the Device Acts as an SSH Client and the Authentication Type is Publickey

Network requirements

As shown in Figure 1-24, establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name is client001 and the SSH server's IP address is 10.165.87.136. Publickey authentication is required.

Figure 1-24 Network diagram of SSH client configuration when using publickey authentication



Configuration procedure

Note

In public key authentication, you can use either RSA or DSA public key. Here takes the DSA public key as an example.

- Configure Switch B

Create a VLAN interface on the device and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<device> system-view
[device] interface vlan-interface 1
[device-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[device-Vlan-interface1] quit
```

Generate RSA and DSA key pairs.

```
[device] public-key local create rsa
[device] public-key local create dsa
```

Set the authentication mode for the user interfaces to AAA.

```
[device] user-interface vty 0 4
[device-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[device-ui-vty0-4] protocol inbound ssh
```

Set the user command privilege level to 3.

```
[device-ui-vty0-4] user privilege level 3
[device-ui-vty0-4] quit
```

Specify the authentication type of user client001 as publickey.

```
[device] ssh user client001 authentication-type publickey
```

 **Note**

Before doing the following steps, you must first generate a DSA public key pair on the client and save the key pair in a file named Switch001, and then upload the file to the SSH server through FTP or TFTP. For details, refer to “Configure Switch A”.

Import the client public key pair named Switch001 from the file Switch001.

```
[device] public-key peer Switch001 import sshkey Switch001
```

Assign the public key Switch001 to user client001.

```
[device] ssh user client001 assign rsa-key Switch001
```

- Configure Switch A

Create a VLAN interface on the device and assign an IP address, which serves as the SSH client’s address in an SSH connection.

```
<device> system-view
[device] interface vlan-interface 1
[device-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[device-Vlan-interface1] quit
```

Generate a DSA key pair

```
[device] public-key local create dsa
```

Export the generated DSA key pair to a file named Switch001.

```
[device] public-key local export dsa ssh2 Switch001
```

Note

After the key pair is generated, you need to upload the pubic key file to the server through FTP or TFTP and complete the server end configuration before you continue to configure the client.

Establish an SSH connection to the server 10.165.87.136.

```
[device] ssh2 10.165.87.136 identity-key dsa
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):n

**************************************************************************
*  Copyright(c) 2004-2009 3Com Corp. and its licensors. All rights reserved.   *
*  Without the owner's prior written consent,                                  *
*  no decompiling or reverse-engineering shall be allowed.                     *
**************************************************************************

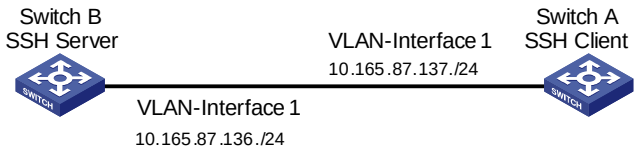
<device>
```

When the Device Acts as an SSH Client and First-time authentication is not Supported

Network requirements

As shown in Figure 1-25, establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name is client001 and the SSH server's IP address is 10.165.87.136. The **publickey** authentication mode is used to enhance security.

Figure 1-25 Network diagram of SSH client configuration



Configuration procedure

- Configure Switch B

Create a VLAN interface on the device and assign an IP address for it to serve as the destination of the client.

```
<device> system-view
[device] interface vlan-interface 1
[device-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
```

```
[device-Vlan-interface1] quit
```

Generate RSA and DSA key pairs.

```
[device] public-key local create rsa
[device] public-key local create dsa
```

Set AAA authentication on user interfaces.

```
[device] user-interface vty 0 4
[device-ui-vty0-4] authentication-mode scheme
```

Configure the user interfaces to support SSH.

```
[device-ui-vty0-4] protocol inbound ssh
```

Set the user command privilege level to 3.

```
[device-ui-vty0-4] user privilege level 3
[device-ui-vty0-4] quit
```

Specify the authentication type for user client001 as publickey.

```
[device] ssh user client001 authentication-type publickey
```

 **Note**

Before doing the following steps, you must first generate a DSA key pair on the client and save the key pair in a file named Switch001, and then upload the file to the SSH server through FTP or TFTP. For details, refer to the following “Configure Switch A”.

Import the client’s public key file Switch001 and name the public key as Switch001.

```
[device] public-key peer Switch001 import sshkey Switch001
```

Assign public key Switch001 to user client001

```
[device] ssh user client001 assign rsa-key Switch001
```

Export the generated DSA host public key pair to a file named Switch002.

```
[device] public-key local export dsa ssh2 Switch002
```

 **Note**

When first-time authentication is not supported, you must first generate a DSA key pair on the server and save the key pair in a file named Switch002, and then upload the file to the SSH client through FTP or TFTP.

- Configure Switch A

Create a VLAN interface on the device and assign an IP address, which serves as the SSH client’s address in an SSH connection.

```
<device> system-view
[device] interface vlan-interface 1
```

```
[device-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[device-Vlan-interface1] quit
```

Generate a DSA key pair

```
[device] public-key local create dsa
```

Export the generated DSA key pair to a file named Switch001.

```
[device] public-key local export dsa ssh2 Switch001
```

Note

After generating the key pair, you need to upload the key pair file to the server through FTP or TFTP and complete the server end configuration before you continue to configure the client.

Disable first-time authentication on the device.

```
[device] undo ssh client first-time
```

Note

When first-time authentication is not supported, you must first generate a DSA key pair on the server and save the key pair in a file named Switch002, and then upload the file to the SSH client through FTP or TFTP. For details, refer to the above part “Configure Switch B”.

Import the public key pair named Switch002 from the file Switch002.

```
[device] public-key peer Switch002 import sshkey Switch002
```

Specify the host public key pair name of the server.

```
[device] ssh client 10.165.87.136 assign rsa-key Switch002
```

Establish the SSH connection to server 10.165.87.136.

```
[device] ssh2 10.165.87.136 identity-key dsa
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

******************************************************************************
*  Copyright(c) 2004-2009 3Com Corp. and its licensors. All rights reserved.   *
*  Without the owner's prior written consent,                                  *
*  no decompiling or reverse-engineering shall be allowed.                     *
******************************************************************************

<device>
```

Table of Contents

1 File System Management Configuration 1-1
File System Configuration 1-1
Introduction to File System 1-1
File System Configuration Tasks 1-1
Directory Operations 1-1
File Operations 1-2
Flash Memory Operations 1-3
Prompt Mode Configuration 1-3
File System Configuration Example 1-4
File Attribute Configuration 1-5
Introduction to File Attributes 1-5
Configuring File Attributes 1-6

1 File System Management Configuration

Note

The sample output information in this manual was created on the WX3024. The output information on your device may vary.

File System Configuration

Introduction to File System

To facilitate management on the device memory, the device provides the file system function, allowing you to access and manage the files and directories. You can create, remove, copy or delete a file through command lines, and you can manage files using directories.

File System Configuration Tasks

Complete the following tasks to configure the file system:

Task	Remarks
Directory Operations	Optional
File Operations	Optional
Flash Memory Operations	Optional
Prompt Mode Configuration	Optional

Note

The device allows you to input a file path and file name in one of the following ways:

- In universal resource locator (URL) format and starting with “unit1>flash:/”. or “flash:/” This method is used to specify a file in the current flash memory.
- Entering the path name or file name directly. This method can be used to specify a path or a file in the current work directory.

Directory Operations

The file system provides directory-related functions, such as:

- Creating/deleting a directory

- Displaying the current work directory, or contents in a specified directory

Follow these steps to perform directory-related operations in user view:

To do…	Use the command…	Remarks
Create a directory	**mkdir** *directory*	Optional
Delete a directory	**rmdir** *directory*	Optional
Display the current work directory	**pwd**	Optional
Display the information about specific directories and files	**dir** [**/all**] [*file-url*]	Optional
Enter a specified directory	**cd** *directory*	Optional

Note

- Only empty directories can be deleted by using the **rmdir** command.
- In the output information of the **dir** /**all** command, deleted files (that is, those stored in the recycle bin) are embraced in brackets.

File Operations

The file system also provides file-related functions listed in the following table.

Follow these steps to perform file operations in user view (except the **execute** command that should be executed in system view):

To do…	Use the command…	Remarks
Delete a file	**delete** [**/unreserved**] *file-url* **delete** { **running-files** | **standby-files** } [**/unreserved**]	Optional A deleted file can be restored by using the **undelete** command if you delete it by executing the **delete** command without specifying the **/unreserved** keyword.
Restore a file in the recycle bin	**undelete** *file-url*	Optional
Delete a file from the recycle bin	**reset recycle-bin** [*file-url*] [**/force**]	Optional
Rename a file	**rename** *fileurl-source fileurl-dest*	Optional
Copy a file	**copy** *fileurl-source fileurl-dest*	Optional
Move a file	**move** *fileurl-source fileurl-dest*	Optional
Display the content of a file	**more** *file-url*	Optional Currently, the file system only supports displaying the contents of text files.
Display the information about a directory or a file	**dir** [**/all**] [*file-url*]	Optional

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Execute the specified batch file	**execute** *filename*	Optional This command should be executed in system view.

Caution

- For deleted files whose names are the same, only the latest deleted file is kept in the recycle bin and can be restored.
- The files which are deleted by the **delete** command without the **/unreserved** keyword are actually moved to the recycle bin and thus still take storage space. You can clear the recycle bin by using the **reset recycle-bin** command.
- The **dir /all** command displays the files in the recycle bin in square brackets.
- If the configuration files are deleted, the device adopts the null configuration when it starts up next time.

Flash Memory Operations

Follow these steps to perform operations on the flash memory in user view:

To do…	Use the command…	Remarks
Format the flash memory	**format** *device*	Required
Restore space on the flash memory	**fixdisk** *device*	Required

Caution

The format operation leads to the loss of all files, including the configuration files, on the flash memory and is irretrievable.

Prompt Mode Configuration

You can set the prompt mode of the current file system to **alert** or **quiet**. In alert mode, the file system will give a prompt for confirmation if you execute a command which may cause data loss, for example, deleting or overwriting a file. In quiet mode, such prompt will not be displayed.

Follow these steps to perform configuration on prompt mode of file system:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the prompt mode of the file system	**file prompt** { **alert** | **quiet** }	Required By default, the prompt mode of the file system is **alert**.

File System Configuration Example

Display all the files in the root directory of the file system.

```
<device> dir /all
Directory of unit1>flash:/

   1       -rw-      1443  Apr 02 2000 02:45:13   startup.cfg
   2       -rwh       151  Apr 02 2000 00:05:53   private-data.txt
   3 (*)   -rw-      1713  Apr 01 2000 23:57:11   vrpcfg.cfg
   4       -rwh       356  Apr 02 2000 03:20:25   dsakey
   5       -rwh       428  Apr 02 2000 03:21:59   hostkey
   6       -rwh       572  Apr 02 2000 03:22:21   serverkey

6858 KB total (6848 KB free)

(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute
```

Copy the file flash:/startup.cfg to flash:/test/, with 1.cfg as the name of the new file.

```
<device> copy flash:/startup.cfg flash:/test/1.cfg
Copy unit1>flash:/startup.cfg to unit1>flash:/test/1.cfg?[Y/N]:y
..
%Copy file unit1>flash:/startup.cfg to unit1>flash:/test/1.cfg...Done.
```

Display the file information after the copy operation.

```
<device>dir /all
Directory of unit1>flash:/

   1       -rw-      1443  Apr 02 2000 02:45:13   startup.cfg
   2       -rwh       151  Apr 02 2000 00:05:53   private-data.txt
   3 (*)   -rw-      1713  Apr 01 2000 23:57:11   vrpcfg.cfg
   4       -rwh       356  Apr 02 2000 03:20:25   dsakey
   5       -rwh       428  Apr 02 2000 03:21:59   hostkey
   6       -rwh       572  Apr 02 2000 03:22:21   serverkey
   7       drw-       -    Apr 02 2000 00:15:8     test

6858 KB total (6848 KB free)

(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute
```

```
<device> dir unit1>flash:/test/
Directory of unit1>flash:/test/

   1       -rw-      1443  Apr 02 2000 02:45:13   1.cfg

6858 KB total (6841 KB free)

(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute
```

File Attribute Configuration

Introduction to File Attributes

The following two startup files support file attribute configuration:

- Configuration files: A configuration file is used to store and restore configuration, with .cfg as the extension.
- Web files: A Web file is used for Web-based network management, with .web as the extension.

The configuration files and Web files support three kinds of attributes: main, backup and none, as described in Table 1-1.

Table 1-1 Description on the file attributes

Attribute	Description	Feature	Identifier
main	Identifies main startup files. The main startup file is used first for the device to start up.	In the flash memory, there can be only one configuration file and one Web file with the main attribute.	(*)
backup	Identifies backup startup files. The backup startup file is used after the device fails to start up using the main startup file.	In the flash memory, there can be only one configuration file and one Web file with the backup attribute.	(b)
none	Identifies files that are neither of main attribute nor backup attribute.	—	None

Note

A file can have both the main and backup attributes. Files of this kind are labeled *b.

Note that, there can be only one configuration file and one Web file with the main attribute in the flash memory. If a newly created file is configured to be with the main attribute, the existing file with the main attribute in the flash memory will lose its main attribute. This circumstance also applies to the file with the backup attribute in the flash memory.

File operations and file attribute operations are independent. For example, if you delete a file with the main attribute from the flash memory, the other files in the flash memory will not possess the main

attribute. If you download a valid file with the same name as the deleted file to the flash memory, the file will possess the main attribute.

Configuring File Attributes

You can configure and view the main attribute or backup attribute of the startup file used for the next startup of a switch, and change the main or backup attribute of the file.

Follow these steps to configure file attributes:

To do…	Use the command…	Remarks
Configure the Web file and its attribute	**boot web-package** *webfile* { **backup** | **main** }	Optional Available in user view
Switch the file attributes between main and backup	**boot attribute-switch** { **all** | **app** | **configuration** | **web** }	Optional Available in user view
Display the information about the app file used as the startup file	**display boot-loader** [**unit** *unit-id*]	Optional Available in any view
Display information about the Web file used by the device	**display web package**	

Caution

- Before configuring the main or backup attribute for a file, make sure the file already exists on the device.
- The configuration of the main or backup attribute of a Web file takes effect immediately without restarting the switch.
- After upgrading a Web file, you need to specify the new Web file in the Boot menu after restarting the device or specify a new Web file by using the **boot web-package** command. Otherwise, Web server cannot function normally.
- Currently, a configuration file has the extension of cfg and resides in the root directory of the flash memory.
- For the detailed configuration of configuration file attributes, refer to the *Configuration File Management* module in this manual.

Table of Contents

1 FTP and SFTP Configuration 1-1
Introduction to FTP and SFTP 1-1
Introduction to FTP 1-1
Introduction to SFTP 1-2
FTP Configuration 1-2
FTP Configuration: The Device Operating as an FTP Server 1-2
FTP Configuration: The Device Operating as an FTP Client 1-6
Configuration Example: The Device Operating as an FTP Server 1-8
FTP Banner Display Configuration Example 1-10
FTP Configuration: The Device Operating as an FTP Client 1-11
SFTP Configuration 1-13
SFTP Configuration: The Device Operating as an SFTP Server 1-13
SFTP Configuration: The Device Operating as an SFTP Client 1-14
SFTP Configuration Example 1-16
2 TFTP Configuration 2-1
Introduction to TFTP 2-1
TFTP Configuration 2-1
TFTP Configuration: The Device Operating as a TFTP Client 2-2
TFTP Configuration Example 2-3

1 FTP and SFTP Configuration

Note

- The term switch used throughout this document refers to a switching device in a generic sense or the switching engine of a WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.
- FTP banner is newly added. For details, see Configuring the banner for an FTP server.

Introduction to FTP and SFTP

Introduction to FTP

FTP (file transfer protocol) is commonly used in IP-based networks to transmit files. Before World Wide Web comes into being, files are transferred through command lines, and the most popular application is FTP. At present, although E-mail and Web are the usual methods for file transmission, FTP still has its strongholds.

As an application layer protocol, FTP is used for file transfer between remote server and local client. FTP uses TCP ports 20 and 21 for data transfer and control command transfer respectively. Basic FTP operations are described in RFC 959.

FTP-based file transmission is performed in the following two modes:

- Binary mode for program file transfer
- ASCII mode for text file transfer

The device can act as an FTP client or the FTP server in FTP-employed data transmission:

Table 1-1 Roles that the device acts as in FTP

Item	Description	Remarks
FTP server	The device can operate as an FTP server to provide file transmission services for FTP clients. You can log in to the device operating as an FTP server by running an FTP client program on your PC to access files on the FTP server.	The prerequisite is that a route exists between the device and the PC.
FTP client	In this case, you need to establish a connection between your PC and the device through a terminal emulation program or Telnet, execute the **ftp** X.X.X.X command on your PC. (X.X.X.X is the IP address of an FTP server or a host name), and enter your user name and password in turn. The device can operate as an FTP client, through which you can access files on the FTP server.	

Introduction to SFTP

Secure FTP (SFTP) is established based on an SSH2 connection. It allows a remote user to log in to the switching engine to manage and transmit files, providing a securer guarantee for data transmission. In addition, since the device can be used as a client, you can log in to remote devices to transfer files securely.

FTP Configuration

Complete the following tasks to configure FTP:

Task		Remarks
FTP Configuration: The Device Operating as an FTP Server	Creating an FTP user	Required
	Enabling an FTP server	Required
	Configuring connection idle time	Optional
	Specifying the source interface and source IP address for an FTP server	Optional
	Disconnecting a specified user	Optional
	Configuring the banner for an FTP server	Optional
	Displaying FTP server information	Optional
FTP Configuration: The Device Operating as an FTP Client	Basic configurations on an FTP client	—
	Specifying the source interface and source IP address for an FTP client	Optional

FTP Configuration: The Device Operating as an FTP Server

Creating an FTP user

Configure the user name and password for the FTP user and set the service type to FTP. To use FTP services, a user must provide a user name and password for being authenticated by the FTP server. Only users that pass the authentication have access to the FTP server.

Follow these steps to create an FTP user:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Add a local user and enter local user view	**local-user** *user-name*	Required By default, no local user is configured.
Configure a password for the specified user	**password** { **simple** | **cipher** } *password*	Optional By default, no password is configured.
Configure the service type as FTP	**service-type ftp**	Required By default, no service is configured.

Enabling an FTP server

Follow these steps to enable an FTP server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the FTP server function	**ftp server enable**	Required Disabled by default.

Note

- Only one user can access the device at a given time when the latter operates as an FTP server.
- Operating as an FTP server, the device cannot receive a file whose size exceeds its storage space. The clients that attempt to upload such a file will be disconnected with the FTP server due to lack of storage space on the FTP server.

Note

To protect unused sockets against attacks, the device provides the following functions:

- TCP 21 is enabled only when you start the FTP server.
- TCP 21 is disabled when you shut down the FTP server.

Configuring connection idle time

After the idle time is configured, if the server does not receive service requests from a client within a specified time period, it terminates the connection with the client, thus preventing a user from occupying the connection for a long time without performing any operation.

Follow these steps to configure connection idle time:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the connection idle time for the FTP server	**ftp timeout** *minutes*	Optional 30 minutes by default

Specifying the source interface and source IP address for an FTP server

You can specify the source interface and source IP address for an FTP server to enhance server security. After this configuration, FTP clients can access this server only through the IP address of the specified interface or the specified IP address.

Note

Source interface refers to the existing VLAN interface or Loopback interface on the device. Source IP address refers to the IP address configured for the interface on the device. Each source interface corresponds to a source IP address. Therefore, specifying a source interface for the FTP server is the same as specifying the IP address of this interface as the source IP address.

Follow these steps to specify the source interface and source IP address for an FTP server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify the source interface for an FTP server	**ftp-server source-interface** *interface-type interface-number*	Use either command Not specified by default.
Specifying the source IP address for an FTP server	**ftp-server source-ip** *ip-address*	

Note

- The specified interface must be an existing one. Otherwise a prompt appears to show that the configuration fails.
- The value of the *ip-address* argument must be an IP address on the device where the configuration is performed. Otherwise a prompt appears to show that the configuration fails.
- You can specify only one source interface or source IP address for the FTP at one time. That is, only one of the commands **ftp-server source-interface** and **ftp-server source-ip** can be valid at one time. If you execute both of them, the new setting will overwrite the original one.
- If the device (FTP server) is the command device or member device in a cluster, do not use the **ftp-server source-ip** command to specify the private IP address of the cluster as the source IP address of the FTP server. Otherwise, FTP does not take effect.

Disconnecting a specified user

On the FTP server, you can disconnect a specified user from the FTP server to secure the network.

Follow these steps to disconnect a specified user:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
On the FTP server, disconnect a specified user from the FTP server	**ftp disconnect** *user-name*	Required

Note

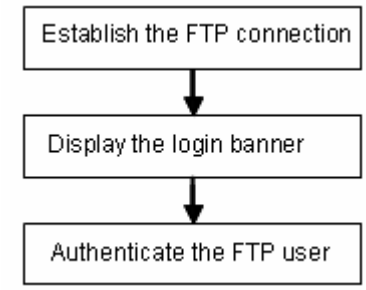
With the device acting as the FTP server, if a network administrator attempts to disconnect a user that is uploading/downloading data to/from the FTP server the device will disconnect the user after the data transmission is completed.

Configuring the banner for an FTP server

Displaying a banner: With a banner configured on the FTP server, when you access the FTP server through FTP, the configured banner is displayed on the FTP client. Banner falls into the following two types:

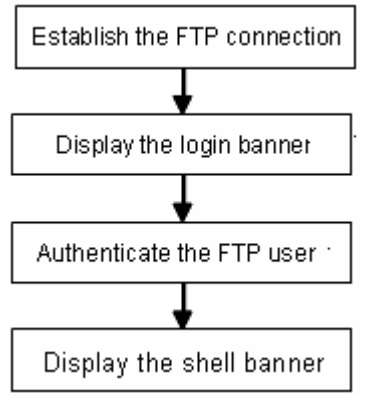
- Login banner: After the connection between an FTP client and an FTP server is established, the FTP server outputs the configured login banner to the FTP client terminal.

Figure 1-1 Process of displaying a login banner



- Shell banner: After the connection between an FTP client and an FTP server is established and correct user name and password are provided, the FTP server outputs the configured shell banner to the FTP client terminal.

Figure 1-2 Process of displaying a shell banner



Follow these steps to configure the banner display for an FTP server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a login banner	**header login** *text*	Required

To do…	Use the command…	Remarks
Configure a shell banner	**header shell** *text*	Use either command or both. By default, no banner is configured.

Note

For details about the **header** command, refer to the Login part of the manual.

Displaying FTP server information

To do…	Use the command…	Remarks
Display the information about FTP server configurations on the device	**display ftp-server**	Available in any view
Display the source IP address set for an FTP server	**display ftp-server source-ip**	
Display the login FTP client on an FTP server	**display ftp-user**	

FTP Configuration: The Device Operating as an FTP Client

Basic configurations on an FTP client

By default the device can operate as an FTP client In this case you can connect the device to the FTP server to perform FTP-related operations (such as creating/removing a directory) by executing commands on the device.

Follow these steps to perform basic configurations on an FTP client:

To do…	Use the command…	Remarks
Enter FTP client view	**ftp** [**cluster** | *remote-server* [*port-number*]]	—
Specify to transfer files in ASCII characters	**ascii**	Use either command By default, files are transferred in ASCII characters.
Specify to transfer files in binary streams	**binary**	
Set the data transfer mode to passive	**passive**	Optional **passive** by default.

To do…	Use the command…	Remarks
Change the working directory on the remote FTP server	**cd** *pathname*	Optional
Change the working directory to be the parent directory	**cdup**	
Get the local working path on the FTP client	**lcd**	
Display the working directory on the FTP server	**pwd**	
Create a directory on the remote FTP server	**mkdir** *pathname*	
Remove a directory on the remote FTP server	**rmdir** *pathname*	
Delete a specified file	**delete** *remotefile*	
Query a specified file on the FTP server	**dir** [*remotefile*] [*localfile*]	Optional If no file name is specified, all the files in the current directory are displayed. The difference between these two commands is that the **dir** command can display the file name, directory as well as file attributes; while the **ls** command can display only the file name and directory.
	ls [*remotefile*] [*localfile*]	
Download a remote file from the FTP server	**get** *remotefile* [*localfile*]	Optional
Upload a local file to the remote FTP server	**put** *localfile* [*remotefile*]	
Rename a file on the remote server	**rename** *remote-source remote-dest*	
Log in with the specified user name and password	**user** *username* [*password*]	
Connect to a remote FTP server	**open** { *ip-address* | *server-name* } [*port*]	
Terminate the current FTP connection without exiting FTP client view	**disconnect**	
	close	
Terminate the current FTP connection and return to user view	**quit**	
	bye	
Display the online help about a specified command concerning FTP	**remotehelp** [*protocol-command*]	
Enable the verbose function	**verbose**	Optional Enabled by default

Specifying the source interface and source IP address for an FTP client

You can specify the source interface and source IP address for the device acting as an FTP client, so that it can connect to a remote FTP server.

Follow these steps to specify the source interface and source IP address for an FTP client:

To do…	Use the command…	Remarks
Specify the source interface used for the current connection	**ftp** { **cluster** | *remote-server* } **source-interface** *interface-type interface-number*	Optional
Specify the source IP address used for the current connection	**ftp** { **cluster** | *remote-server* } **source-ip** *ip-address*	Optional
Enter system view	**system-view**	—
Specify an interface as the source interface the FTP client uses every time it connects to an FTP server	**ftp source-interface** *interface-type interface-number*	Use either command Not specified by default
Specify an IP address as the source IP address the FTP client uses every time it connects to an FTP server	**ftp source-ip** *ip-address*	
Display the source IP address used by an FTP client every time it connects to an FTP server	**display ftp source-ip**	Available in any view

Note

- The specified interface must be an existing one. Otherwise a prompt appears to show that the configuration fails.
- The value of the *ip-address* argument must be the IP address of the device where the configuration is performed. Otherwise a prompt appears to show that the configuration fails.
- The source interface/source IP address set for one connection is prior to the fixed source interface/source IP address set for each connection. That is, for a connection between an FTP client and an FTP server, if you specify the source interface/source IP address used for the connection this time, and the specified source interface/source IP address is different from the fixed one, the former will be used for the connection this time.
- Only one fixed source interface or source IP address can be set for the FTP client at one time. That is, only one of the commands **ftp source-interface** and **ftp source-ip** can be valid at one time. If you execute both of them, the new setting will overwrite the original one.

Configuration Example: The Device Operating as an FTP Server

Network requirements

As shown in Figure 1-3, the switching engine operates as an FTP server and a remote PC as an FTP client. The configuration file **config.cfg** of the switching engine is stored on the PC. Upload the configuration file to the remote switching engine through FTP and use the **startup**

saved-configuration command to specify **config.cfg** as the main configuration file for next startup and then reboot the device.

- Create a user account on the FTP server with the user name “switch” and password “hello”.
- The IP addresses 1.1.1.1 for a VLAN interface on the switching engine and 2.2.2.2 for the PC have been configured. Ensure that a route exists between the device and the PC.

Figure 1-3 Network diagram for FTP configurations: the device operating as an FTP server



Configuration procedure

1) Configure Switch A (the FTP server)

Log in to the switching engine and enable the FTP server function on the switching engine. Configure the user name and password used to access FTP services, and specify the service type as FTP (You can log in to the switching engine through the console port or by telnetting the switching engine. See the “Login” module for detailed information.)

Configure the FTP user name as “switch”, the password as “hello”, and the service type as FTP.

```
<device>
<device> system-view
[device] ftp server enable
[device] local-user switch
[device-luser-switch] password simple hello
[device-luser-switch] service-type ftp
```

2) Configure the PC (FTP client)

Run an FTP client application on the PC to connect to the FTP server. Upload the configuration file named **config.cfg** to the root directory of the flash memory of the FTP server. The following takes the command line window tool provided by Windows as an example:

Enter the command line window and switch to the directory where the file **config.cfg** is located. In this example it is in the root directory of C:\.

```
C:\>
```

Access the switching engine through FTP. Input the user name “switch” and password “hello” to log in and enter FTP view.

```
C:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User (1.1.1.1:(none)): switch
331 Password required for switch.
Password:
230 User logged in.
ftp>
```

Upload the **config.cfg** file.

```
ftp> put config.cfg
```

```
200 Port command okay.
150 Opening ASCII mode data connection for config.cfg.
226 Transfer complete.
```

This example uses the command line window tool provided by Windows. When you log in to the FTP server through another FTP client, refer to the corresponding instructions for operation description.

Caution

- If available space on the flash memory of the device is not enough to hold the file to be uploaded, you need to delete files not in use from the flash memory to make room for the file, and then upload the file again. The files in use cannot be deleted.
- The device is not shipped with FTP client application software. You need to purchase and install it by yourself.

---

3) Configure Switch A (FTP server)

After uploading the configuration file, use the **startup saved-configuration** command to specify the uploaded configuration file as the main configuration file for next startup, and restart the device.

```
<device>startup saved-configuration config.cfg main
 Please wait.....................................Done!
```

Note

For information about the **startup saved-configuration** command and how to specify the main configuration file for the switching engine, refer to the System Maintenance and Debugging part of this manual.

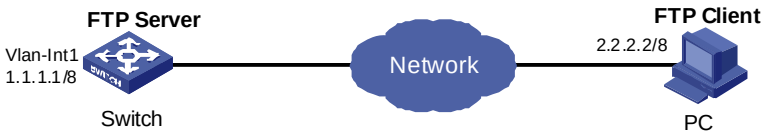
FTP Banner Display Configuration Example

Network requirements

As shown in Figure 1-4, configure the device as an FTP server and the remote PC as an FTP client. After a connection between the FTP client and the FTP server is established and login succeeds, the banner is displayed on the FTP client.

- An FTP user named “switch” and the password “hello” have been configured on the FTP server.
- The IP addresses 1.1.1.1 for a VLAN interface on the switching engine and 2.2.2.2 for the PC have been configured. Ensure that a route exists between the device and the PC.
- Configure the login banner of the switching engine as “login banner appears” and the shell banner as “shell banner appears”.

Figure 1-4 Network diagram for FTP banner display configuration



Configuration procedure

1) Configure the switch (FTP server)

Configure the login banner of the switching engine as “login banner appears” and the shell banner as “shell banner appears”. For detailed configuration of other network requirements, see Configuration Example: The Device Operating as an FTP Server.

```
<device> system-view
[device] header login %login banner appears%
[device] header shell %shell banner appears%
[device]
```

2) Configure the PC (FTP client)

Access the switching engine through FTP. Enter the user name “switch“ and the password “hello” to log in to the device, and then enter FTP view. Login banner appears after FTP connection is established. Shell banner appears after the user passes the authentication.

```
C:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220-login banner appears

220 FTP service ready.
User (1.1.1.1:(none)): switch
331 Password required for switch.
Password:
230-shell banner appears

230 User logged in.
ftp>
```

FTP Configuration: The Device Operating as an FTP Client

Network requirements

As shown in Figure 1-5, the device operates as an FTP client and a remote PC as an FTP server. The configuration file of the switching engine named **config.cfg** is stored on the PC. Download it to the switching engine through FTP and use the **startup saved-configuration** command to specify **config.cfg** as the main configuration file for next startup, and then reboot the device.

- Create a user account on the FTP server with the user name “switch” and password “hello”, and grant the user “switch” read and write permissions for the directory named “Switch” on the PC.
- Configure the IP address 1.1.1.1 for a VLAN interface on the device, and 2.2.2.2 for the PC. Ensure a route exists between the device and the PC.

Figure 1-5 Network diagram for FTP configurations: the device operating as an FTP client



Configuration procedure

1) Configure the PC (FTP server)

Perform FTP server–related configurations on the PC, that is, create a user account on the FTP server with user name “switch” and password “hello”. (For detailed configuration, refer to the configuration instruction relevant to the FTP server software.)

2) Configure the switch (FTP client)

Log in to the switching engine. (You can log in to the switching engine through the console port or by telnetting the switching engine. See the “Login” module for detailed information.)

Caution

If available space on the flash memory of the device is not enough to hold the file to be uploaded, you need to delete files not in use from the flash memory to make room for the file, and then upload the file again. The files in use cannot be deleted.

Connect to the FTP server using the **ftp** command in user view. You need to provide the IP address of the FTP server, the user name and the password as well to enter FTP view.

```
<device> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 FTP service ready.
User(none):switch
331 Password required for switch.
Password:
230 User logged in.
[ftp]
```

Enter the authorized directory on the FTP server.

```
[ftp] cd switch
```

Execute the **put** command to upload the configuration file named **config.cfg** to the FTP server.

```
[ftp] put config.cfg
```

Execute the **get** command to download the file named **config.cfg** to the flash memory of the device.

```
[ftp] get config.cfg
```

Execute the **quit** command to terminate the FTP connection and return to user view.

```
[ftp] quit
```

```
<device>
```

After downloading the file, use the **startup saved-configuration** command to specify the downloaded configuration file as the main configuration file for next startup, and then restart the device.

```
<device>startup saved-configuration config.cfg main
 Please wait.....................................Done!
```



Note

For information about the **startup saved-configuration** command and how to specify the startup file for the device, refer to the “System Maintenance and Debugging” module of this manual.

SFTP Configuration

Complete the following tasks to configure SFTP:

Task		Remarks
SFTP Configuration: The Device Operating as an SFTP Server	Enabling an SFTP server	Required
	Configuring connection idle time	Optional
	Supported SFTP client software	—
SFTP Configuration: The Device Operating as an SFTP Client	Basic configurations on an SFTP client	—
	Specifying the source interface or source IP address for an SFTP client	Optional

SFTP Configuration: The Device Operating as an SFTP Server

Enabling an SFTP server

Before enabling an SFTP server, you need to enable the SSH server function and specify the service type of the SSH user as **SFTP** or **all**. For details, see the SSH server configuration part of *SSH Operation Manual* of this manual.

Follow these steps to enable an SFTP server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable an SFTP server	**sftp server enable**	Required Disabled by default

Configuring connection idle time

After the idle time is configured, if the server does not receive service requests from a client within a specified time period, it terminates the connection with the client, thus preventing a user from occupying the connection for a long time without performing any operation.

Follow these steps to configure connection idle time:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the connection idle time for the SFTP server	**ftp timeout** *time-out-value*	Optional 10 minutes by default

Supported SFTP client software

The device operating as an SFTP server can interoperate with SFTP client software, including SSH Tectia Client v4.2.0 (SFTP), v5.0, and WINSCP.

SFTP client software supports the following operations: logging in to a device; uploading a file; downloading a file; creating a directory; modify a file name or a directory name; browsing directory structure; and manually terminating a connection.

For configurations on client software, see the corresponding configuration manual.

Note

- Currently the device operating as an SFTP server supports the connection of only one SFTP user. When multiple users attempt to log in to the SFTP server or multiple connections are enabled on a client, only the first user can log in to the SFTP user. The subsequent connection will fail.
- When you upload a large file through WINSCP, if a file with the same name exists on the server, you are recommended to set the packet timeout time to over 600 seconds, thus to prevent the client from failing to respond to device packets due to timeout. Similarly, when you delete a large file from the server, you are recommended to set the client packet timeout time to over 600 seconds.

SFTP Configuration: The Device Operating as an SFTP Client

Basic configurations on an SFTP client

By default the device can operate as an SFTP client. In this case you can connect the device to the SFTP server to perform SFTP-related operations (such as creating/removing a directory) by executing commands on the device.

Follow these steps to perform basic configurations on an SFTP client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Enter SFTP client view	**sftp** { *host-ip* | *host-name* } [*port-num*] [**identity-key** { **dsa** | **rsa** } | **prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128** } | **prefer_stoc_cipher** { **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *	Required
Change the working directory on the remote SFTP server	**cd** *pathname*	Optional
Change the working directory to be the parent directory	**cdup**	
Display the working directory on the SFTP server	**pwd**	
Create a directory on the remote SFTP server	**mkdir** *pathname*	
Remove a directory on the remote SFTP server	**rmdir** *pathname*	
Delete a specified file	**delete** *remotefile*	Optional
	remove *remote-file*	Both commands have the same effect.
Query a specified file on the SFTP server	**dir** [*remotefile*] [*localfile*]	Optional
	ls [*remotefile*] [*localfile*]	If no file name is provided, all the files in the current directory are displayed. The difference between these two commands is that the **dir** command can display the file name, directory as well as file attributes; while the **ls** command can display only the file name and directory.
Download a remote file from the SFTP server	**get** *remotefile* [*localfile*]	Optional
Upload a local file to the remote SFTP server	**put** *localfile* [*remotefile*]	
Rename a file on the remote server	**rename** *remote-source remote-dest*	
Exit SFTP client view and return to system view	**bye**	The three commands have the same effect.
	exit	
	quit	
Display the online help about a specified command concerning SFTP	**help** [**all** | *command-name*]	Optional

Note

If you specify to authenticate a client through public key on the server, the client needs to read the local private key when logging in to the SFTP server. Since both RSA and DSA are available for public key authentication, you need to use the **identity-key** key word to specify the algorithms to get correct local private key; otherwise you will fail to log in. For details, see *SSH Operation*.

Specifying the source interface or source IP address for an SFTP client

You can specify the source interface or source IP address for the device acting as an FTP client, so that it can connect to a remote SFTP server.

Follow these steps to specify the source interface or source IP address for an SFTP client:

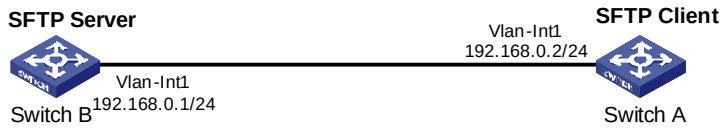
To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify an interface as the source interface of the specified SFTP client	**sftp source-interface** *interface-type interface-number*	Use either command Not specified by default
Specify an IP address as the source IP address of the specified SFTP client	**sftp source-ip** *ip-address*	
Display the source IP address used by the current SFTP client	**display sftp source-ip**	Optional Available in any view.

SFTP Configuration Example

Network requirements

As shown in Figure 1-6, establish an SSH connection between the SFTP client (Switch A) and the SFTP server (switch B). Log in to Switch B through switch A to manage and transmit files. An SFTP user account with the user name **client001** and password **abc** exists on the SFTP server.

Figure 1-6 Network diagram for SFTP configuration



Configuration procedure

1) Configure the SFTP server (Switch B)

Create key pairs.

```
<device> system-view
[device] public-key local create rsa
[device] public-key local create dsa
```

Create a VLAN interface on the device and assign to it an IP address, which is used as the destination address for the client to connect to the SFTP server.

```
[device] interface vlan-interface 1
[device-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[device-Vlan-interface1] quit
```

Specify the SSH authentication mode as AAA.

```
[device] user-interface vty 0 4
[device-ui-vty0-4] authentication-mode scheme
```

Configure the protocol through which the remote user logs in to the device as SSH.

```
[device-ui-vty0-4] protocol inbound ssh
[device-ui-vty0-4] quit
```

Create a local user client001.

```
[device] local-user client001
[device-luser-client001] password simple abc
[device-luser-client001] service-type ssh
[device-luser-client001] quit
```

Configure the authentication mode as **password**. Authentication timeout time, retry number, and update time of the server key adopt the default values.

```
[device] ssh user client001 authentication-type password
```

Specify the service type as SFTP.

```
[device] ssh user client001 service-type sftp
```

Enable the SFTP server.

```
[device] sftp server enable
```

2) Configure the SFTP client (Switch A)

Configure the IP address of the VLAN interface on Switch A. It must be in the same segment with the IP address of the VLAN interface on Switch B. In this example, configure it as 192.168.0.2.

```
<device> system-view
[device] interface vlan-interface 1
[device-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[device-Vlan-interface1] quit
```

Connect to the remote SFTP server. Enter the user name “client001” and the password “abc”, and then enter SFTP client view.

```
[device] sftp 192.168.0.1
Input Username: client001
Trying 192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):n
Enter password:
```

```
sftp-client>
```

Display the current directory of the server. Delete the file z and verify the result.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
-rwxrwxrwx   1 noone    nogroup         0 Sep 01 08:00 z
Received status: End of file
Received status: Success
sftp-client> delete z
The following files will be deleted:
/z
Are you sure to delete it?(Y/N):y
This operation may take a long time.Please wait...

Received status: Success
File successfully Removed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
Received status: End of file
Received status: Success
```

Add a directory new1, and then check whether the new directory is successfully created.

```
sftp-client> mkdir new1
Received status: Success
New directory created
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:30 new1
Received status: End of file
Received status: Success
```

Rename the directory new1 as new2, and then verify the result.

```
sftp-client> rename new1 new2
File successfully renamed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
```

```
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
Received status: End of file
Received status: Success
```

Download the file pubkey2 from the server and rename it as public.

```
sftp-client> get pubkey2 public
This operation may take a long time, please wait...
.
Remote  file:/pubkey2 --->  Local file: public..
Received status: End of file
Received status: Success
Downloading file successfully ended
```

Upload the file pu to the server and rename it as puk, and then verify the result.

```
sftp-client> put pu puk
This operation may take a long time, please wait...
Local file: pu --->  Remote file: /puk
Received status: Success
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:36 puk
Received status: End of file
Received status: Success
sftp-client>
```

Exit SFTP.

```
sftp-client> quit
Bye
[device]
```

2 TFTP Configuration

Introduction to TFTP

Compared with FTP, TFTP (trivial file transfer protocol) features simple interactive access interface and no authentication control. Therefore, TFTP is applicable in the networks where client-server interactions are relatively simple. TFTP is implemented based on UDP. It transfers data through UDP port 69. Basic TFTP operations are described in RFC 1986.

TFTP transmission is initiated by clients, as described in the following:

- To download a file, a client sends Read Request packets to the TFTP server, then receives data from the TFTP server, and sends acknowledgement packets to the TFTP server.
- To upload a file, a client sends Write Request packets to the TFTP server, then sends data to the TFTP server, and receives acknowledgement packets from the TFTP server.

The device can act as a TFTP client only.

When you download a file that is larger than the free space of the device's flash memory:

- If the TFTP server supports file size negotiation, file size negotiation will be initiated between the device and the server and the file download operation will be aborted if the free space of the device's flash memory is found to be insufficient.
- If the TFTP server does not support file size negotiation, the device will receive data from the server until the flash memory is full. If there is more data to be downloaded, the device will prompt that the space is insufficient and delete the data partially downloaded. File download fails.

TFTP-based file transmission can be performed in the following modes:

- Binary mode for program file transfer.
- ASCII mode for text file transfer.

Note

Before performing TFTP-related configurations, you need to configure IP addresses for the TFTP client and the TFTP server, and make sure a route exists between the two.

TFTP Configuration

Complete the following tasks to configure TFTP:

Task		Remarks
TFTP Configuration: The Device Operating as a TFTP Client	Basic configurations on a TFTP client	—
	Specifying the source interface or source IP address for an FTP client	Optional

Task		Remarks
TFTP server configuration	For details, see the corresponding manual	—

TFTP Configuration: The Device Operating as a TFTP Client

Basic configurations on a TFTP client

By default the device can operate as a TFTP client. In this case you can connect the device to the TFTP server to perform TFTP-related operations (such as creating/removing a directory) by executing commands on the device.

Follow these steps to perform basic configurations on a TFTP client:

To do…	Use the command…	Remarks
Download a file from a TFTP server	**tftp** *tftp-server* **get** *source-file* [*dest-file*]	Optional
Upload a file to a TFTP server	**tftp** *tftp-server* **put** *source-file* [*dest-file*]	Optional
Enter system view	**system-view**	—
Set the file transmission mode	**tftp** { **ascii** | **binary** }	Optional Binary by default
Specify an ACL rule used by the specified TFTP client to access a TFTP server	**tftp-server acl** *acl-number*	Optional Not specified by default

Specifying the source interface or source IP address for an FTP client

You can specify the source interface and source IP address for the device operating as a TFTP client, so that it can connect with a remote TFTP server through the IP address of the specified interface or the specified IP address.

Follow these steps to specify the source interface and source IP address for a TFTP client:

To do…	Use the command…	Remarks
Specify the source interface used for the current connection	**tftp** *tftp-server* **source-interface** *interface-type interface-number* { **get** *source-file* [*dest-file*] | **put** *source-file-url* [*dest-file*] }	Optional Not specified by default
Specify the source IP address used for the current connection	**tftp** *tftp-server* **source-ip** *ip-address* { **get** *source-file* [*dest-file*] | **put** *source-file-url* [*dest-file*] }	Optional Not specified by default
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Specify an interface as the source interface a TFTP client uses every time it connects to a TFTP server	**tftp source-interface** *interface-type interface-number*	Use either command Not specified by default
Specify an IP address as the source IP address a TFTP client uses every time it connects to a TFTP server	**tftp source-ip** *ip-address*	
Display the source IP address used by a TFTP client every time it connects to a TFTP server	**display tftp source-ip**	Optional Available in any view

Note

- The specified interface must be an existing one; otherwise a prompt appears to show that the configuration fails.
- The value of the *ip-address* argument must be an IP address on the device where the configuration is performed, and otherwise a prompt appears to show that the configuration fails.
- The source interface/source IP address set for one connection is prior to the fixed source interface/source IP address set for each connection. That is, for a connection between a TFTP client and a TFTP server, if you specify the source interface/source IP address only used for the connection this time, and the specified source interface/source IP address is different from the fixed one, the former will be used for the connection this time.
- You may specify only one source interface or source IP address for the TFTP client at one time. That is, only one of the commands **tftp source-interface** and **tftp source-ip** can be effective at one time. If both commands are configured, the one configured later will overwrite the original one.

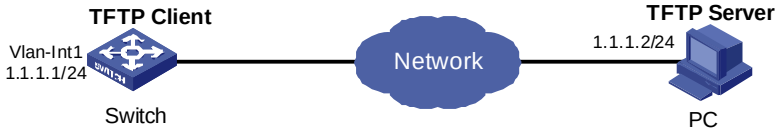
TFTP Configuration Example

Network requirements

As shown in Figure 2-1, the device operates as a TFTP client and a PC as the TFTP server. The configuration file named **config.cfg** is stored on the PC. Download it to the device through TFTP, and use the **startup saved-configuration** command to specify **config.cfg** as the main configuration file for next startup.

- The TFTP working directory is configured on the TFTP server.
- Configure the IP addresses of a VLAN interface on the device and the PC as 1.1.1.1 and 1.1.1.2 respectively. The port through which the device connects with the PC belongs to the VLAN.

Figure 2-1 Network diagram for TFTP configurations



Configuration procedure

1) Configure the TFTP server (PC)

Start the TFTP server and configure the working directory on the PC.

2) Configure the TFTP client (switch).

Log in to the switching engine. (You can log in to the switching engine through the console port or by telnetting the device. See the “Login” module for detailed information.)

Caution

If available space on the flash memory of the device is not enough to hold the file to be uploaded, you need to delete files not in use from the flash memory to make room for the file, and then upload the file again. The files in use cannot be deleted.

Enter system view

```
<device> system-view
[device]
```

Configure the IP address of a VLAN interface on the device to be 1.1.1.1, and ensure that the port through which the device connects with the PC belongs to this VLAN. (This example assumes that the port belongs to VLAN 1.)

```
[device] interface Vlan-interface 1
[device-Vlan-interface1] ip address 1.1.1.1 255.255.255.0
[device-Vlan-interface1] quit
```

Download the device configuration file named **config.cfg** from the TFTP server to the device.

```
<device> tftp 1.1.1.2 get config.cfg config.cfg
```

After downloading the file, use the **startup saved-configuration** command to specify the downloaded configuration file as the main configuration file for next startup, and restart the device.

```
<device>startup saved-configuration config.cfg main
 Please wait.....................................Done!
```

Note

For information about the **startup saved-configuration** command and how to specify the startup file for the device, refer to *System Maintenance and Debugging Operation* of this manual and *System Maintenance and Debugging Command* in the accompanying command manual.

Table of Contents

1 Information Center 1-1
Information Center Overview 1-1
Introduction to Information Center 1-1
System Information Format 1-4
Information Center Configuration 1-6
Introduction to the Information Center Configuration Tasks 1-6
Configuring Synchronous Information Output 1-7
Configuring to Display the Time Stamp with the UTC Time Zone 1-7
Setting to Output System Information to the Console 1-8
Setting to Output System Information to a Monitor Terminal 1-10
Setting to Output System Information to a Log Host 1-11
Setting to Output System Information to the Trap Buffer 1-12
Setting to Output System Information to the Log Buffer 1-12
Setting to Output System Information to the SNMP NMS 1-13
Displaying and Maintaining Information Center 1-14
Information Center Configuration Examples 1-14
Log Output to a UNIX Log Host 1-14
Log Output to a Linux Log Host 1-16
Log Output to the Console 1-17
Configuration Example 1-18

1 Information Center

Note

- The term switch used throughout this document refers to a switching device in a generic sense or the switching engine of a WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Information Center Overview

Introduction to Information Center

Acting as the system information hub, information center classifies and manages system information. Together with the debugging function (the **debugging** command), information center offers a powerful support for network administrators and developers in monitoring network performance and diagnosing network problems.

The information center of the system has the following features:

Classification of system information

The system is available with three types of information:

- Log information
- Trap information
- Debugging information

Eight levels of system information

The information is classified into eight levels by severity and can be filtered by level. More emergent information has a smaller severity level.

Table 1-1 Severity description

Severity	Severity value	Description
emergencies	1	The system is unavailable.
alerts	2	Information that demands prompt reaction
critical	3	Critical information
errors	4	Error information
warnings	5	Warnings
notifications	6	Normal information that needs to be noticed

Severity	Severity value	Description
informational	7	Informational information to be recorded
debugging	8	Information generated during debugging

Information filtering by severity works this way: information with the severity value greater than the configured threshold is not output during the filtering.

- If the threshold is set to 1, only information with the severity being emergencies will be output;
- If the threshold is set to 8, information of all severities will be output.

Ten channels and six output directions of system information

The system supports six information output directions, including the Console, Monitor terminal (monitor), logbuffer, loghost, trapbuffer and SNMP.

The system supports ten channels. The channels 0 through 5 have their default channel names and are associated with six output directions by default. Both the channel names and the associations between the channels and output directions can be changed through commands.

Table 1-2 Information channels and output directions

Information channel number	Default channel name	Default output direction
0	console	Console (Receives log, trap and debugging information)
1	monitor	Monitor terminal (Receives log, trap and debugging information, facilitating remote maintenance)
2	loghost	Log host (Receives log, trap and debugging information and information will be stored in files for future retrieval.)
3	trapbuffer	Trap buffer (Receives trap information, a buffer inside the device for recording information.)
4	logbuffer	Log buffer (Receives log information, a buffer inside the device for recording information.)
5	snmpagent	SNMP NMS (Receives trap information)
6	channel6	Not specified (Receives log, trap, and debugging information)
7	channel7	Not specified (Receives log, trap, and debugging information)
8	channel8	Not specified (Receives log, trap, and debugging information)
9	channel9	Not specified (Receives log, trap, and debugging information)

Note

Configurations for the six output directions function independently and take effect only after the information center is enabled.

Outputting system information by source module

The system information can be classified by source module and then filtered. Some module names and description are shown in Table 1-3.

Table 1-3 Source module name list

Module name	Description
8021X	802.1x module
ACL	Access control list module
ADBM	Address base module
AM	Access management module
ARP	Address resolution protocol module
CMD	Command line module
DEV	Device management module
DNS	Domain name system module
ETH	Ethernet module
FIB	Forwarding module
FTM	Fabric topology management module
FTPS	FTP server module
HA	High availability module
HABP	Huawei authentication bypass protocol module
HTTPD	HTTP server module
HWCM	Huawei Configuration Management private MIB module
HWP	HWPing module
IFNET	Interface management module
IGSP	IGMP snooping module
IP	Internet protocol module
LAGG	Link aggregation module
LINE	Terminal line module
MSTP	Multiple spanning tree protocol module
NAT	Network address translation module
NDP	Neighbor discovery protocol module
NTDP	Network topology discovery protocol module

Module name	Description
NTP	Network time protocol module
PKI	Public key infrastructure module
RDS	Radius module
RMON	Remote monitor module
RSA	Revest, Shamir and Adleman encryption module
SHELL	User interface module
SNMP	Simple network management protocol module
SOCKET	Socket module
SSH	Secure shell module
SYSMIB	System MIB module
TAC	HWTACACS module
TELNET	Telnet module
TFTPC	TFTP client module
VLAN	Virtual local area network module
VTY	Virtual type terminal module
XM	XMODEM module
default	Default settings for all the modules

To sum up, the major task of the information center is to output the three types of information of the modules onto the ten channels in terms of the eight severity levels and according to the user's settings, and then redirect the system information from the ten channels to the six output directions.

System Information Format

System information has the following format:

```
<priority> timestamp sysname module/level/digest:content
```

Note

- The closing set of angel brackets < >, the space, the forward slash /, and the colon are all required in the above format.
- Before the <priority> may have %, "#, or * followed with a space, indicating log, alarm, or debugging information respectively.

Below is an example of the format of log information to be output to a log host:

```
% <188>Dec  6 10:44:55:283 2006 device NTP/5/NTP_LOG:- 1 - NTP service enable
```

("-1-" indicates that the unit number of the device is 1.)

What follows is a detailed explanation of the fields involved:

Priority

The priority is calculated using the following formula: facility*8+severity-1, in which

- facility (the device name) defaults to local7 with the value being 23 (the value of local6 is 22, that of local5 is 21, and so on).
- severity (the information level) ranges from 1 to 8. Table 1-1 details the value and meaning associated with each severity.

Note that there is no space between the priority and timestamp fields and the priority field appears only when the information has been sent to the log host.

Timestamp

Timestamp records the time when system information is generated to allow users to check and identify system events.

Note that there is a space between the timestamp and sysname (host name) fields.

The time stamp has the following two formats.

1) Without the universal time coordinated (UTC) time zone, the time stamp is in the format of “Mmm dd hh:mm:ss:ms yyyy”.
2) With the UTC time zone, the time stamp is in the format of “Mmm dd hh:mm:ss:ms yyyy [GMT +|- hh:mm:ss]”.

Each field is described as follows:

- “Mmm” represents the month, and the available values are: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
- “dd” is the date, which shall follow a space if less than 10, for example, “ 7”.
- “hh:mm:ss:ms” is the local time, where “hh” is in the 24-hour format, ranging from 00 to 23, both “mm” and ”ss” range from 00 to 59, “ms” ranges from 000 to 999.
- “yyyy” is the year.
- “[GMT +|- hh:mm:ss]” is the UTC time zone, which represents the time difference with the Greenwich standard time.

Because devices in a network may distribute in different time zones, when the time displayed in the time stamps of output information is the local time on each device, it is not so convenient for you to locate and solve problems globally. In this case, you can configure the information center to add UTC time zone to the time stamp of the output information, so that you can know the standard time when the information center processing each piece of information. That is, you can know the Greenwich standard time of each device in the network based on the UTC record in the time stamp.

To add UTC time zone to the time stamp in the information center output information, you must:

- Set the local time zone
- Set the time stamp format in the output direction of the information center to **date**
- Configure to add UTC time zone to the output information

After the above configuration, the UTC time zone will be displayed in the output information, like the following:

```
%Dec  8 10:12:21:708 2006 [GMT+08:00:00] device SHELL/5/LOGIN:- 1 - VTY(1.1.0.2) in unit1
login
```

Sysname

Sysname is the system name of the local device and defaults to **device**.

You can use the **sysname** command to modify the system name. Refer to the System Maintenance and Debugging part of this manual for details)

Note that there is a space between the sysname and module fields.

Module

The module field represents the name of the module that generates system information. You can enter the **info-center source ?** command in system view to view the module list. Refer to Table 1-3 for module name and description.

Between “module” and “level” is a “/”.

Level (Severity)

System information can be divided into eight levels based on its severity, from 1 to 8. Refer to Table 1-1 for definition and description of these severity levels. Note that there is a forward slash “/” between the level (severity) and digest fields.

Digest

The digest field is a string of up to 32 characters, outlining the system information.

Note that there is a colon between the digest and content fields.

Content

This field provides the content of the system information.

Note

The above section describes the log information format sent to a log host by the device. Some log host software will resolve the received information as well as its format, so that you may see the log format displayed on the log host is different from the one described in this manual.

Information Center Configuration

Introduction to the Information Center Configuration Tasks

Complete the following tasks to configure the information center:

Task	Remarks
Configuring Synchronous Information Output	Optional
Configuring to Display the Time Stamp with the UTC Time Zone	Optional
Setting to Output System Information to the Console	Optional
Setting to Output System Information to a Monitor Terminal	Optional
Setting to Output System Information to a Log Host	Optional
Setting to Output System Information to the Trap Buffer	Optional
Setting to Output System Information to the Log Buffer	Optional

Task	Remarks
Setting to Output System Information to the SNMP NMS	Optional

Configuring Synchronous Information Output

Synchronous information output refers to the feature that if the system information such as log, trap, or debugging information is output when the user is inputting commands, the command line prompt (in command editing mode a prompt, or a [Y/N] string in interaction mode) and the input information are echoed after the output.

This feature is used in the case that your input is interrupted by a large amount of system output. With this feature enabled, the system echoes your previous input and you can continue your operations from where you were stopped.

Follow these steps to configure synchronous information output:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable synchronous information output	**info-center synchronous**	Required Disabled by default

Note

- If the system information is output before you input any information following the current command line prompt, the system does not echo any command line prompt after the system information output.
- In the interaction mode, you are prompted for some information input. If the input is interrupted by system output, no system prompt (except the Y/N string) will be echoed after the output, but your input will be displayed in a new line.

Configuring to Display the Time Stamp with the UTC Time Zone

To add UTC time zone to the time stamp in the information center output information, you must:

- Set the local time zone
- Set the time stamp format in the output direction of the information center to **date**
- Configure to add the UTC time zone to the output information

Follow these steps to configure to display time stamp with the UTC time zone:

To do…	Use the command…	Remarks
Set the time zone for the system	**clock timezone** *zone-name* { **add** | **minus** } *time*	Required By default, UTC time zone is set for the system.
Enter system view	**system-view**	—

To do…		Use the command…	Remarks
Set the time stamp format in the output direction of the information center to **date**	Log host direction	**info-center timestamp loghost date**	Required Use either command
	Non log host direction	**info-center timestamp** { **log** | **trap** | **debugging** } **date**	
Set to display the UTC time zone in the output information of the information center		**info-center timestamp utc**	Required By default, no UTC time zone is displayed in the output information

Setting to Output System Information to the Console

Setting to output system information to the console

Follow these steps to set to output system information to the console:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.
Enable system information output to the console	**info-center console channel** { *channel-number* | *channel-name* }	Optional By default, the device uses information channel 0 to output log/debugging/trap information to the console.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	**info-center timestamp { log | trap | debugging } { boot | date | none }**	Optional By default, the time stamp format of the log and trap output information is **date**, and that of the debugging output information is **boot**.

Note

To view the debugging information of some modules on the device, you need to set the type of the output information to **debug** when configuring the system information output rules, and use the **debugging** command to enable debugging for the corresponding modules.

Table 1-4 Default output rules for different output directions

Output direction	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/disabled	Severity	Enabled/disabled	Severity	Enabled/disabled	Severity
Console	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging
Monitor terminal	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging
Log host	default (all modules)	Enabled	informational	Enabled	debugging	Disabled	debugging
Trap buffer	default (all modules)	Disabled	informational	Enabled	warnings	Disabled	debugging
Log buffer	default (all modules)	Enabled	warnings	Disabled	debugging	Disabled	debugging
SNMP NMS	default (all modules)	Disabled	debugging	Enabled	warnings	Disabled	debugging

Enabling system information display on the console

After setting to output system information to the console, you need to enable the associated display function to display the output information on the console.

Follow these steps to enable the system information display on the console:

To do…	Use the command…	Remarks
Enable the debugging/log/trap information terminal display function	**terminal monitor**	Optional Enabled by default.
Enable debugging information terminal display function	**terminal debugging**	Optional Disabled by default.
Enable log information terminal display function	**terminal logging**	Optional Enabled by default.
Enable trap information terminal display function	**terminal trapping**	Optional Enabled by default.

Note

Make sure that the debugging/log/trap information terminal display function is enabled (use the **terminal monitor** command) before you enable the corresponding terminal display function by using the **terminal debugging**, **terminal logging**, or **terminal trapping** command.

Setting to Output System Information to a Monitor Terminal

System information can also be output to a monitor terminal, which is a user terminal that has login connections through the AUX, VTY, or TTY user interface.

Setting to output system information to a monitor terminal

Follow these steps to set to output system information to a monitor terminal:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.
Enable system information output to Telnet terminal or dumb terminal	**info-center monitor channel** { *channel-number* | *channel-name* }	Optional By default, the device outputs log/debugging/trap information to a user terminal through information channel 1.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional By default, the time stamp format of the log and trap output information is **date**, and that of the debugging output information is **boot**.

Note

- When there are multiple Telnet users or dumb terminal users, they share some configuration parameters including module filter, language and severity level threshold. In this case, change to any such parameter made by one user will also be reflected on all other user terminals.
- To view debugging information of specific modules, you need to set the information type as **debug** when setting the system information output rules, and enable debugging for corresponding modules through the **debugging** command.

Enabling system information display on a monitor terminal

After setting to output system information to a monitor terminal, you need to enable the associated display function in order to display the output information on the monitor terminal.

Follow these steps to enable the display of system information on a monitor terminal:

To do…	Use the command…	Remarks
Enable the debugging/log/trap information terminal display function	**terminal monitor**	Optional Enabled by default
Enable debugging information terminal display function	**terminal debugging**	Optional Disabled by default
Enable log information terminal display function	**terminal logging**	Optional Enabled by default
Enable trap information terminal display function	**terminal trapping**	Optional Enabled by default



Note

Make sure that the debugging/log/trap information terminal display function is enabled (use the **terminal monitor** command) before you enable the corresponding terminal display function by using the **terminal debugging**, **terminal logging**, or **terminal trapping** command.

Setting to Output System Information to a Log Host

Follow these steps to set to output system information to a log host:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.
Enable system information output to a log host	**info-center loghost** *host-ip-addr* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number*]*	Required By default, the device does not output information to the log host. After you configure the device to output information to the log host, the device uses information channel 2 by default.
Configure the source interface through which log information is sent to the log host	**info-center loghost source** *interface-type interface-number*	Optional By default, no source interface is configured, and the system automatically selects an interface as the source interface.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.

To do…	Use the command…	Remarks
Set the format of the time stamp to be sent to the log host	**info-center timestamp loghost** { **date** | **no-year-date** | **none** }	Optional By default, the time stamp format of the information output to the log host is **date**.

Note

Be sure to set the correct IP address when using the **info-center loghost** command. A loopback IP address will cause an error message prompting that this address is invalid.

Setting to Output System Information to the Trap Buffer

Follow these steps to set to output system information to the trap buffer:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.
Enable system information output to the trap buffer	**info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]*	Optional By default, the device uses information channel 3 to output trap information to the trap buffer, which can holds up to 256 items by default.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	**info-center timestamp** { **log | trap** | **debugging** } { **boot** | **date** | **none** }	Optional By default, the time stamp format of the output trap information is **date**.

Setting to Output System Information to the Log Buffer

Follow these steps to set to output system information to the log buffer:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.

To do…	Use the command…	Remarks
Enable information output to the log buffer	**info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]*	Optional By default, the device uses information channel 4 to output log information to the log buffer, which can holds up to 512 items by default.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional By default, the time stamp format of the output log information is **date**.

Setting to Output System Information to the SNMP NMS

Follow these steps to set to output system information to the SNMP NMS:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.
Enable information output to the SNMP NMS	**info-center snmp channel** { *channel-number* | *channel-name* }	Optional By default, the device outputs trap information to SNMP through channel 5.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional By default, the time stamp format of the information output to the SNMP NMS is **date**.



Note

To send information to a remote SNMP NMS properly, related configurations are required on both the device and the SNMP NMS.

Displaying and Maintaining Information Center

To do…	Use the command…	Remarks
Display information on an information channel	**display channel** [*channel-number* | *channel-name*]	Available in any view
Display the operation status of information center, the configuration of information channels, the format of time stamp	**display info-center** [**unit** *unit-id*]	
Display the status of log buffer and the information recorded in the log buffer	**display logbuffer** [**unit** *unit-id*] [**level** *severity* | **size** *buffersize*]* [| { **begin** | **exclude** | **include** } *regular-expression*]	
Display the summary information recorded in the log buffer	**display logbuffer summary** [**level** *severity*]	
Display the status of trap buffer and the information recorded in the trap buffer	**display trapbuffer** [**unit** *unit-id*] [**size** *buffersize*]	
Clear information recorded in the log buffer	**reset logbuffer** [**unit** *unit-id*]	Available in user view
Clear information recorded in the trap buffer	**reset trapbuffer** [**unit** *unit-id*]	

Information Center Configuration Examples

Log Output to a UNIX Log Host

Network requirements

As shown in Figure 1-1, Switch sends the following log information to the Unix log host whose IP address is 202.38.1.10: the log information of the two modules ARP and IP, with severity higher than “informational”.

Figure 1-1 Network diagram for log output to a Unix log host



Configuration procedure

1) Configure Switch:

Enable the information center.

```
<Switch> system-view
[Switch] info-center enable
```

Disable the function of outputting information to log host channels.

```
[Switch] undo info-center source default channel loghost
```

Configure the host whose IP address is 202.38.1.10 as the log host. Permit ARP and IP modules to output information with severity level higher than informational to the log host.

```
[Switch] info-center loghost 202.38.1.10 facility local4
[Switch] info-center source arp channel loghost log level informational debug state off trap state off
[Switch] info-center source ip channel loghost log level informational debug state off trap state off
```

2) Configure the log host:

The operations here are performed on SunOS 4.0. The operations on other manufacturers' Unix operation systems are similar.

Step 1: Execute the following commands as the super user (root user).

```
# mkdir /var/log/Switch
# touch /var/log/Switch/information
```

Step 2: Edit the file "/etc/syslog.conf" as the super user (root user) to add the following selector/action pairs.

```
# Switch configuration messages
local4.info    /var/log/Switch/information
```

Note

When you edit the file "/etc/syslog.conf", note that:

- A note must start in a new line, starting with a "#" sign.
- In each pair, a tab should be used as a separator instead of a space.
- No space is allowed at the end of a file name.
- The device name (facility) and received log information severity level specified in the file "/etc/syslog.conf" must be the same as those corresponding parameters configured in the commands **info-center loghost** and **info-center source**. Otherwise, log information may not be output to the log host normally.

Step 3: After the log file "information" is created and the file "/etc/syslog.conf" is modified, execute the following command to send a HUP signal to the system daemon "syslogd", so that it can reread its configuration file "/etc/syslog.conf".

```
# ps -ae | grep syslogd
147
# kill -HUP 147
```

After all the above operations, the device can make records in the corresponding log file.

Note

Through combined configuration of the device name (facility), information severity level threshold (severity), module name (filter) and the file “syslog.conf”, you can sort information precisely for filtering.

Log Output to a Linux Log Host

Network requirements

As shown in Figure 1-2, Switch sends the following log information to the Linux log host whose IP address is 202.38.1.10: All modules' log information, with severity higher than “errors”.

Figure 1-2 Network diagram for log output to a Linux log host



Configuration procedure

1) Configure Switch:

Enable the information center.

```
<Switch> system-view
[Switch] info-center enable
```

Configure the host whose IP address is 202.38.1.10 as the log host. Permit all modules to output log information with severity level higher than error to the log host.

```
[Switch] info-center loghost 202.38.1.10 facility local7
[Switch] info-center source default channel loghost log level errors debug state off trap state off
```

2) Configure the log host:

Step 1: Execute the following commands as a super user (root user).

```
# mkdir /var/log/Switch
# touch /var/log/Switch/information
```

Step 2: Edit the file “/etc/syslog.conf” as the super user (root user) to add the following selector/action pairs.

```
# Switch configuration messages
local7.info    /var/log/Switch/information
```

Note

Note the following items when you edit file “/etc/syslog.conf”.

- A note must start in a new line, starting with a “#" sign.
- In each pair, a tab should be used as a separator instead of a space.
- No space is permitted at the end of the file name.
- The device name (facility) and received log information severity specified in file “/etc/syslog.conf” must be the same with those corresponding parameters configured in commands **info-center loghost** and **info-center source**. Otherwise, log information may not be output to the log host normally.

Step 3: After the log file “information” is created and the file “/etc/syslog.conf” is modified, execute the following commands to view the process ID of the system daemon “syslogd”, stop the process, and then restart the daemon "syslogd" in the background with the “-r” option.

```
# ps -ae | grep syslogd
147
# kill -9 147
# syslogd -r &
```

In case of Linux log host, the daemon “syslogd” must be started with the “-r” option.

After all the above operations, the device can record information in the corresponding log file.

Note

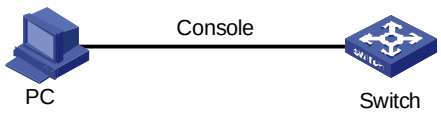
Through combined configuration of the device name (facility), information severity level threshold (severity), module name (filter) and the file “syslog.conf”, you can sort information precisely for filtering.

Log Output to the Console

Network requirements

As shown in Figure 1-3, Switch sends the following information to the console: the log information of the two modules ARP and IP, with severity higher than “informational”.

Figure 1-3 Network diagram for log output to the console



Configuration procedure

Enable the information center.

```
<Switch> system-view
```

```
[Switch] info-center enable
```

Disable the function of outputting information to the console channels.

```
[Switch] undo info-center source default channel console
```

Enable log information output to the console. Permit ARP and IP modules to output log information with severity level higher than informational to the console.

```
[Switch] info-center console channel console
[Switch] info-center source arp channel console log level informational debug state off trap state off
[Switch] info-center source ip channel console log level informational debug state off trap state off
```

Enable terminal display.

```
<Switch> terminal monitor
<Switch> terminal logging
```

Configuration Example

Network requirements

- As shown in Figure 1-4, the device is in the time zone of GMT+ 08:00:00.
- The time stamp format of output log information is date.
- UTC time zone will be added to the output information of the information center.

Figure 1-4 Network diagram



Configuration procedure

Name the local time zone z8 and configure it to be eight hours ahead of UTC time.

```
<Switch> clock timezone z8 add 08:00:00
```

Set the time stamp format of the log information to be output to the log host to date.

```
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch] info-center timestamp loghost date
```

Configure to add UTC time to the output information of the information center.

```
[Switch] info-center timestamp utc
```

Table of Contents

1 Host Configuration File Loading 1-1
Introduction to Loading Approaches 1-1
Remote Loading Using FTP 1-1
Remote Loading Using TFTP 1-5
2 Basic System Configuration and Debugging 2-1
Basic System Configuration 2-1
Displaying the System Status 2-2
Debugging the System 2-2
Enabling/Disabling System Debugging 2-2
Displaying Debugging Status 2-3
Displaying Operating Information about Modules in System 2-3
3 Network Connectivity Test 3-1
Network Connectivity Test 3-1
ping 3-1
tracert 3-1
4 Device Management 4-1
Introduction to Device Management 4-1
Device Management Configuration 4-1
Device Management Configuration Tasks 4-1
Rebooting the Device 4-1
Scheduling a Reboot on the Device 4-2
Configuring Real-time Monitoring of the Running Status of the System 4-2
Specifying the Main Configuration File to be Used at Next Reboot 4-2
Identifying and Diagnosing Pluggable Transceivers 4-3
Displaying and Maintaining the Device Management Configuration 4-4

1 Host Configuration File Loading

Note

- The term switch used throughout this document refers to a switching device in a generic sense or the switching engine of a WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Traditionally, device software is loaded through a serial port. This approach is slow, time-consuming and cannot be used for remote loading. To resolve these problems, the TFTP and FTP modules are introduced into the device. With these modules, you can load/download software/files conveniently to the device through an Ethernet port.

This chapter introduces how to load the host configuration file to the device remotely.

Introduction to Loading Approaches

You can load software remotely by using:

- FTP
- TFTP

If your terminal is not directly connected to the device, you can telnet to the device, and use FTP or TFTP to load the host configuration file remotely.

Remote Loading Using FTP

Loading procedure using FTP client

1) Loading the host configuration file

As shown in Figure 1-1, a PC is used as both the configuration device and the FTP server. You can telnet to Switch, and then execute the FTP commands to download the host configuration file from the remote FTP server (whose IP address is 10.1.1.1) to Switch.

Figure 1-1 Remote loading using FTP Client



Step 1: Download the file to the device using FTP commands.

```
<device> oap connect slot 0
```

```
Connected to OAP!
<device_LSW> ftp 192.168.0.100
Trying ...
Press CTRL+K to abort
Connected.
220 3Com 3CDaemon FTP Server Version 2.0
User(none):admin
331 User name ok, need password
Password:
230 User logged in

[ftp]get config.cfg config.cfg

227 Entering passive mode (192,168,0,100,5,95)
125 Using existing data connection
.........226 Closing data connection; File transfer successful.
FTP: 7590 byte(s) received in 15.139 second(s) 501.00 byte(s)/sec.

[ftp] bye
```

Note

When using different FTP server software on PC, different information will be output to the device.

Step 2: Update the host configuration file on Switch.

```
<device_LSW> startup saved-configuration config.cfg main
 Please wait.....................................Done!
```

Step 3: Restart Switch.

```
<device_LSW> reboot
```

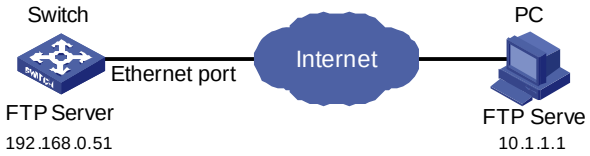
Note

Before restarting Switch, make sure you have saved all other configurations that you want, so as to avoid losing configuration information.

Loading procedure using FTP server

As shown in Figure 1-2, Switch is used as the FTP server. You can telnet to Switch, and then execute the FTP commands to upload the configuration file config.cfg to Switch.

Figure 1-2 Remote loading using FTP server



Step 1: As shown in Figure 1-2, connect Switch through an Ethernet port to the PC (whose IP address is 10.1.1.1)

Step 2: Configure the IP address of VLAN-interface 1 on Switch to 192.168.0.51, and subnet mask to 255.255.255.0.

Note

You can configure the IP address for any VLAN on Switch for FTP transmission. However, before configuring the IP address for a VLAN interface, you have to make sure whether the IP addresses of this VLAN and PC are routable.

```
<device> oap connect slot 0
Connected to OAP!
<device_LSW> system-view
deviceView: return to User View with Ctrl+Z.
[device_LSW]interface Vlan-interface 1
[device_LSW-Vlan-interface1]ip add 192.168.0.51 255.255.255.0
```

Step 3: Enable FTP service on Switch, and configure the FTP user name to test and password to pass.

```
[device_LSW-Vlan-interface1]quit
[device_LSW]ftp server enable
[device_LSW]local-user test
New local user added.
[device_LSW-luser-test]password simple pass
[device_LSW-luser-test]service-type ftp
```

Step 4: Enable FTP client software on the PC. The following takes the command line interface in Windows for illustration.

```
C:\Documents and Settings\Administrator>
```

Step 5: Use the **cd** command on the interface to enter the path that the upgrade file is to be stored. Assume the name of the path is **D:\update**.

```
C:\Documents and Settings\Administrator>d:

D:\>cd update

D:\Update>
```

Step 6: Enter **ftp 192.168.0.51** and enter the user name **test**, password **pass** to log on to the FTP server.

```
C:\Documents and Settings\Administrator>d:

D:\>cd update

D:\Update>ftp 192.168.0.51
Connected to 192.168.0.51.
220 FTP service ready.
User (192.168.0.51:(none)): test
331 Password required for test.
Password:
230 User logged in.

ftp>
```

Step 7: Use the **put** command to upload the file **config.cfg** to Switch.

```
C:\Documents and Settings\Administrator>d:

D:\>cd update

D:\Update>ftp 192.168.0.51
Connected to 192.168.0.51.
220 FTP service ready.
User (192.168.0.51:(none)): test
331 Password required for test.
Password:
230 User logged in.

ftp> put startup.cfg
200 Port command okay.
150 Opening ASCII mode data connection for /startup.cfg.
226 Transfer complete.
```

Step 8: Configure **config.cfg** as the main configuration file at next startup, and then restart Switch.

```
<device_LSW> startup saved-configuration config.cfg main
 Please wait.....................................Done!

<device_LSW> reboot
```

After Switch restarts, the file **config.cfg** is used as the main configuration file. It indicates that the configuration file loading is finished.

Note

- The steps listed above are performed in the Windows operating system, if you use other FTP client software, refer to the corresponding user guide before operation.
- Only the configuration steps concerning loading are listed here. For detailed description on the corresponding configuration commands, refer to the “FTP-SFTP-TFTP” part of this manual.

Remote Loading Using TFTP

The remote loading using TFTP is similar to that using FTP. The only difference is that TFTP is used to load software to Switch, and Switch can only act as a TFTP client.

2 Basic System Configuration and Debugging

Basic System Configuration

Follow these steps to perform basic system configuration:

To do…	Use the command…	Remarks
Set the current date and time of the system	**clock datetime** *HH:MM:SS* { *YYYY/MM/DD* | *MM/DD/YYYY* }	Required Execute this command in user view. The default value is 23:55:00 04/01/2000 when the system starts up.
Set the local time zone	**clock timezone** *zone-name* { **add** | **minus** } *HH:MM:SS*	Optional Execute this command in user view. By default, it is the UTC time zone.
Set the name and time range of the summer time	**clock summer-time** *zone_name* { **one-off** | **repeating** } *start-time start-date end-time end-date offset-time*	Optional Execute this command in user view. • When the system reaches the specified start time, it automatically adds the specified offset to the current time, so as to toggle the system time to the summer time. • When the system reaches the specified end time, it automatically subtracts the specified offset from the current time, so as to toggle the summer time to normal system time.
Enter system view from user view	**system-view**	—
Set the system name of the device	**sysname** *sysname*	Optional By default, the name is **device**.
Return from current view to lower level view	**quit**	Optional If the current view is user view, you will quit the current user interface.
Return from current view to user view	**return**	Optional The composite key **Ctrl+Z** has the same effect with the **return** command.

Displaying the System Status

To do…	Use the command…	Remarks
Display the current date and time of the system	**display clock**	Available in any view
Display the version of the system	**display version**	
Display the information about users logging onto the device	**display users** [**all**]	

Debugging the System

Enabling/Disabling System Debugging

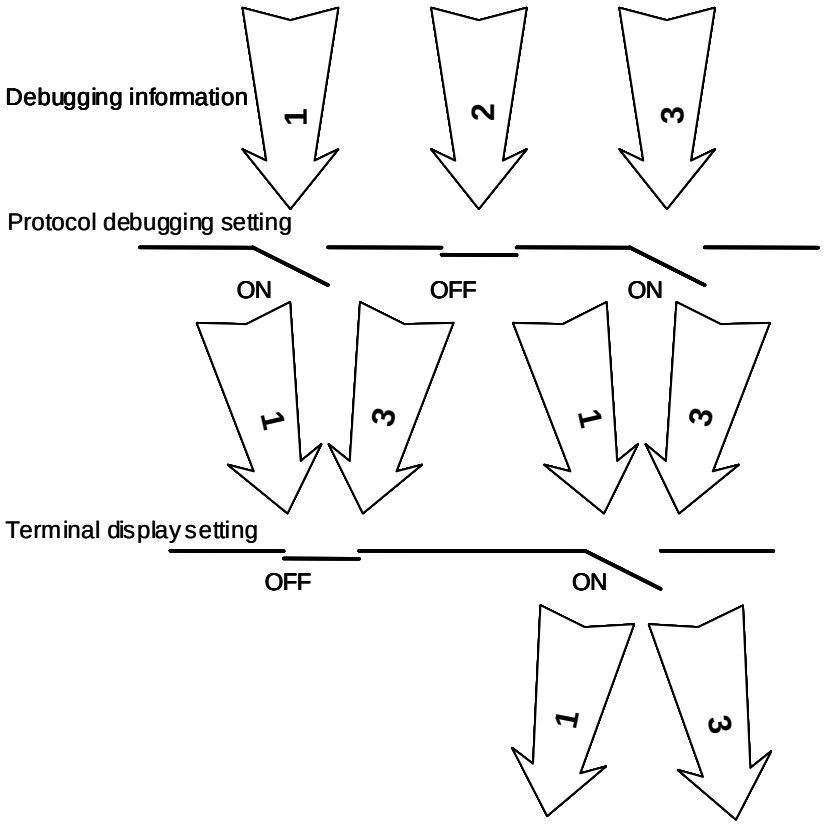
The device provides a variety of debugging functions. Most of the protocols and features supported by the device are provided with corresponding debugging functions. These debugging functions help users diagnose and troubleshoot the system faults.

The output of debugging information is determined by the following two settings:

- Protocol debugging setting, which controls whether the debugging information of a protocol is output.
- Terminal display setting, which controls whether the debugging information is output to the screen of a specific user.

The relationship between the two settings is as follows:

Figure 2-1 Debugging information output



You can use the following commands to enable the two settings.

Follow these steps to enable debugging and terminal display for a specific module:

To do…	Use the command…	Remarks
Enable system debugging for specific module	**debugging** *module-name* [*debugging-option*]	Required Disabled for all modules by default.
Enable terminal display for debugging	**terminal debugging**	Required Disabled by default.

Caution

The output of debugging information affects the system operation. Disable all debugging after you finish the system debugging.

Displaying Debugging Status

Follow these steps to display the current debugging status in the system:

To do…	Use the command…	Remarks
Display all enabled debugging on the current device	**display debugging** [**unit** *unit-id*] [**interface** *interface-type interface-number*] [*module-name*]	You can execute the **display** command in any view.

Displaying Operating Information about Modules in System

When the device is in trouble, you may need to view a lot of operating information to locate the problem. Each functional module has its corresponding operating information display command(s). You can use the command here to display the current operating information about the modules in the system for troubleshooting your system.

Follow these steps to display the current operation information about the modules in the system:

To do…	Use the command…	Remarks
Display the current operation information about the modules in the system.	**display diagnostic-information**	You can use this command in any view. You should execute this command twice to find the difference between the two executing results, thus helping locate the problem.

3 Network Connectivity Test

Network Connectivity Test

ping

You can use the **ping** command to check the network connectivity and the reachability of a host.

Follow these steps to execute the **ping** command:

To do…	Use the command…	Remarks
Check the IP network connectivity and the reachability of a host	**ping** [**-a** *ip-address*] [**-c** *count*] [**-d**] [**-f**] [**-h** *ttl*] [**-i** *interface-type interface-number*] [**ip**] [**-n**] [**- p** *pattern*] [**-q**] [**-s** *packetsize*] [**-t** *timeout*] [**-tos** *tos*] [**-v**] *host*	You can execute this command in any view.

This command can output the following results:

- Response status for each ping packet. If no response packet is received within the timeout time, the message "Request time out" is displayed. Otherwise, the number of data bytes, packet serial number, TTL (time to live) and response time of the response packet are displayed.
- Final statistics, including the numbers of sent packets and received response packets, the irresponsive packet percentage, and the minimum, average and maximum values of response time.

tracert

You can use the **tracert** command to trace the gateways that a packet passes from the source to the destination. This command is mainly used to check the network connectivity. It can also be used to help locate the network faults.

The executing procedure of the **tracert** command is as follows: First, the source host sends a data packet with the TTL of 1, and the first hop device returns an ICMP error message indicating that it cannot forward this packet because of TTL timeout. Then, the source host resends the packet with the TTL of 2, and the second hop device also returns an ICMP TTL timeout message. This procedure goes on and on until the packet gets to the destination. During the procedure, the system records the source address of each ICMP TTL timeout message in order to offer the path that the packet passed through to the destination.

Follow these steps to execute the **tracert** command:

To do…	Use the command…	Remarks
View the gateways that a packet passes from the source host to the destination	**tracert** [**-a** *source-ip*] [**-f** *first-ttl*] [**-m** *max-ttl*] [**-p** *port*] [**-q** *num-packet*] [**-w** *timeout*] *string*	You can execute the **tracert** command in any view.

4 Device Management

Introduction to Device Management

Device Management includes the following:

- Reboot the device
- Configure real-time monitoring of the running status of the system
- Specify the main configuration file to be used at the next reboot

Device Management Configuration

Device Management Configuration Tasks

Complete the following tasks to configure device management:

Task	Remarks
Rebooting the Device	Optional
Scheduling a Reboot on the Device	Optional
Configuring Real-time Monitoring of the Running Status of the System	Optional
Specifying the Main Configuration File to be Used at Next Reboot	Optional
Identifying and Diagnosing Pluggable Transceivers	Optional

Rebooting the Device

You can perform the following operation in user view when the device is faulty or needs to be rebooted.

Note

Before rebooting, the system checks whether there is any configuration change. If yes, it prompts whether or not to proceed. This prevents the system from losing the configurations in case of shutting down the system without saving the configurations.

Follow the step below to reboot the device:

To do…	Use the command…	Remarks
Reboot the device	**reboot** [**unit** *unit-id*]	Available in user view

Scheduling a Reboot on the Device

After you schedule a reboot on the device, the device will reboot at the specified time.

Follow these steps to schedule a reboot on the device:

To do…	Use the command…	Remarks
Schedule a reboot on the device, and set the reboot date and time	**schedule reboot at** *hh:mm* [*mm/dd/yyyy* | *yyyy/mm/dd*]	Optional
Schedule a reboot on the device, and set the delay time for reboot	**schedule reboot delay** { *hh:mm* | *mm* }	Optional
Enter system view	**system-view**	—
Schedule a reboot on the device, and set the reboot period	**schedule reboot regularity at** *hh:mm period*	Optional

Note

The device timer can be set to precision of one minute, that is, the device will reboot within one minute after the specified reboot date and time.

Configuring Real-time Monitoring of the Running Status of the System

This function enables you to dynamically record the system running status, such as CPU, thus facilitating analysis and solution of the problems of the device.

Follow these steps to configure real-time monitoring of the running status of the system:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable real-time monitoring of the running status of the system	**system-monitor enable**	Optional Enabled by default.

Caution

Enabling of this function consumes some amounts of CPU resources. Therefore, if your network has a high CPU usage requirement, you can disable this function to release your CPU resources.

Specifying the Main Configuration File to be Used at Next Reboot

If multiple configuration files exist in the flash memory, you can use the command here to specify the one that will be used when the device reboots.

Follow the step below to specify the main configuration file to be used at reboot:

To do…	Use the command…	Remarks
Specify the main configuration file to be used at next reboot	**startup saved-configuration** *filename* [**main | backup**]	Required

Identifying and Diagnosing Pluggable Transceivers

Introduction to pluggable transceivers

At present, four types of pluggable transceivers are commonly used, and they can be divided into optical transceivers and electrical transceivers based on transmission media as shown in Table 4-1.

Table 4-1 Commonly used pluggable transceivers

Transceiver type	Applied environment	Whether can be an optical transceiver	Whether can be an electrical transceiver
SFP (Small Form-factor Pluggable)	Generally used for 100M/1000M Ethernet interfaces or POS 155M/622M/2.5G interfaces	Yes	Yes
GBIC (GigaBit Interface Converter)	Generally used for 1000M Ethernet interfaces	Yes	Yes
XFP (10-Gigabit small Form-factor Pluggable)	Generally used for 10G Ethernet interfaces	Yes	No
XENPAK (10 Gigabit EtherNet Transceiver Package)	Generally used for 10G Ethernet interfaces	Yes	Yes

Note

For pluggable transceivers supported by the device, refer to *3Com WX3000 Series Unified Switches Installation Manual*.

Identifying pluggable transceivers

As pluggable transceivers are of various types and from different vendors, you can perform the following configurations to identify main parameters of the pluggable transceivers, including transceiver type, connector type, central wavelength of the laser sent, transfer distance and vendor name or vendor name specified.

Follow these steps to identify pluggable transceivers:

To do…	Use the command…	Remarks
Display main parameters of the pluggable transceiver(s)	**display transceiver interface** [*interface-type interface-number*]	Available for all pluggable transceivers

Diagnosing pluggable transceivers

The system outputs alarm information for you to diagnose and troubleshoot faults of pluggable transceivers. When these parameters are abnormal, you can take corresponding measures to prevent transceiver faults.

Follow these steps to display pluggable transceiver information:

To do…	Use the command…	Remarks
Display the current alarm information of the pluggable transceiver(s)	**display transceiver alarm interface** [*interface-type interface-number*]	Available for all pluggable transceivers

Displaying and Maintaining the Device Management Configuration

To do…	Use the command…	Remarks
Display the module type and operating status of each board	**display device** [**manuinfo** | **unit** *unit-id*]	Available in any view
Display CPU usage of the device	**display cpu** [**unit** *unit-id*]	
Display the operating status of the fan	**display fan** [**unit** *unit-id* [*fan-id*]]	
Display memory usage of the device	**display memory** [**unit** *unit-id*]	
Display the operating status of the power supply	**display power** [**unit** *unit-id* [*power-id*]]	
Display system diagnostic information or save system diagnostic information to a file with the extension .diag into the flash memory	**display diagnostic-information**	
Display enabled debugging on the current device	**display debugging** [**unit** *unit-id*] [**interface** *interface-type interface-number*] [*module-name*]	

Table of Contents

1 VLAN-VPN Configuration 1-1
VLAN-VPN Overview 1-1
Introduction to VLAN-VPN 1-1
Implementation of VLAN-VPN 1-2
Adjusting the TPID Values of VLAN-VPN Packets 1-2
VLAN-VPN Configuration 1-3
Configuration Task List 1-3
Enabling the VLAN-VPN Feature for a Port 1-3
TPID Adjusting Configuration 1-4
Displaying and Maintaining VLAN-VPN 1-4
VLAN-VPN Configuration Example 1-5
Transmitting User Packets through a Tunnel in the Public Network by Using VLAN-VPN 1-5
2 Selective QinQ Configuration 2-1
Selective QinQ Overview 2-1
Selective QinQ Overview 2-1
Inner-to-Outer Tag Priority Mapping 2-2
Selective QinQ Configuration 2-2
Configuration Task List 2-2
Enabling the Selective QinQ Feature for a Port 2-2
Configuring the Inner-to-Outer Tag Priority Mapping Feature 2-3
Selective QinQ Configuration Example 2-3
Processing Private Network Packets by Their Types 2-3

1 VLAN-VPN Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

VLAN-VPN Overview

Introduction to VLAN-VPN

Virtual private network (VPN) is a new technology that emerges with the expansion of the Internet. It can be used for establishing private networks over the public network. With VPN, you can specify to process packets on the client or the access end of the service provider in specific ways, establish dedicated tunnels for user traffic on public network devices, and thus improve data security.

VLAN-VPN feature is a simple yet flexible Layer 2 tunneling technology. It tags private network packets with outer VLAN tags, thus enabling the packets to be transmitted through the service providers' backbone networks with both inner and outer VLAN tags. In public networks, packets of this type are transmitted by their outer VLAN tags (that is, the VLAN tags of public networks), and the inner VLAN tags are treated as part of the payload.

Figure 1-1 describes the structure of the packets with single-layer VLAN tags.

Figure 1-1 Structure of packets with single-layer VLAN tags

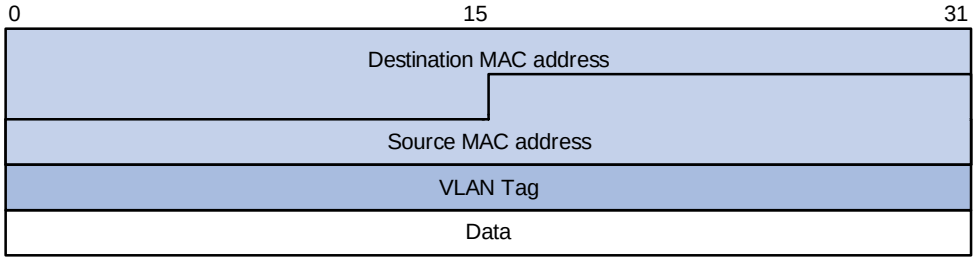
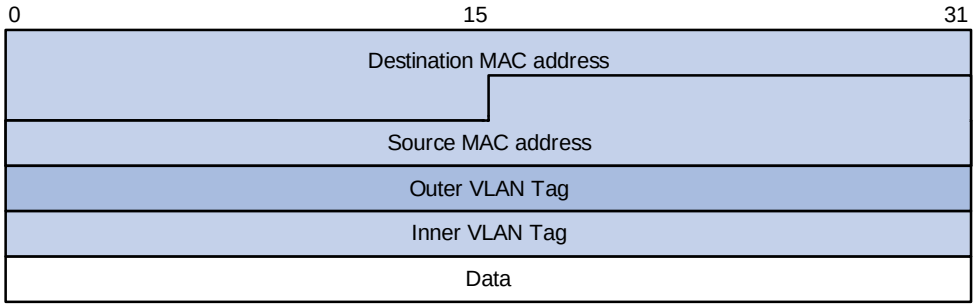


Figure 1-2 describes the structure of the packets with double-layer VLAN tags.

Figure 1-2 Structure of packets with double-layer VLAN tags



Compared with MPLS-based Layer 2 VPN, VLAN-VPN has the following features:

- It provides Layer 2 VPN tunnels that are simpler.
- VLAN-VPN can be implemented through manual configuration. That is, signaling protocol-related configuration is not needed.

The VLAN-VPN feature provides you with the following benefits:

- Saves public network VLAN ID resource.
- You can have VLAN IDs of your own, which is independent of public network VLAN IDs.
- Provides simple Layer 2 VPN solutions for small-sized MANs or intranets.

Implementation of VLAN-VPN

With the VLAN-VPN feature enabled, no matter whether or not a received packet already carries a VLAN tag, the device will tag the received packet with the default VLAN tag of the receiving port and add the source MAC address to the MAC address table of the default VLAN. When a packet reaches a VLAN-VPN-enabled port:

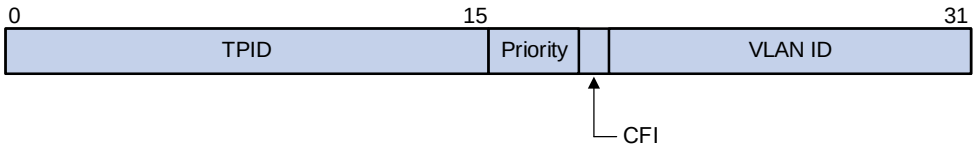
- If the packet already carries a VLAN tag, the packet becomes a dual-tagged packet.
- Otherwise, the packet becomes a packet carrying the default VLAN tag of the port.

Adjusting the TPID Values of VLAN-VPN Packets

Tag protocol identifier (TPID) is a field of the VLAN tag. IEEE 802.1Q specifies the value of TPID to be 0x8100.

Figure 1-3 illustrates the structure of the Tag packet of an Ethernet frame defined by IEEE 802.1Q.

Figure 1-3 The structure of the Tag packet of an Ethernet frame



By default, the device adopts the TPID value (0x8100) specified in the protocol. Some vendors use other TPID values (such as 0x9100).

To be compatible with devices of other vendors, the device can adjust the TPID values of VLAN-VPN packets globally. You can configure TPID values by yourself. When forwarding packets, the VLAN-VPN uplink port sets the TPID value for outer VLAN tags of these packets to the user-defined value, so that these packets forwarded to the public network can be recognized by devices of other vendors.

As the position of the TPID field in an Ethernet packet is the same as that of the upper-layer protocol type field in a packet without VLAN Tag, to avoid confusion in the process of receiving/forwarding a packet, the TPID value cannot be any of the protocol type value listed in Table 1-1.

Table 1-1 Commonly used protocol type values in Ethernet frames

Protocol type	Value
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1x	0x888E

VLAN-VPN Configuration

Configuration Task List

Complete the following tasks to configure VLAN-VPN:

Task	Remarks
Enabling the VLAN-VPN Feature for a Port	Required
TPID Adjusting Configuration	Optional

Enabling the VLAN-VPN Feature for a Port

Configuration Prerequisites

- The port is not a VLAN-VPN uplink port.
- The port is not a remote mirror reflection port.

Configuration procedure

Follow these steps to enable the VLAN-VPN feature for a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the VLAN-VPN feature on the port	**vlan-vpn enable**	Required By default, the VLAN-VPN feature is disabled on a port.

TPID Adjusting Configuration

Configuration Prerequisites

- To change the global TPID value 0x8100, you need to specify a port on the device as a VLAN VPN uplink port. Before the configuration, make sure that VLAN VPN is disabled on the port.
- For proper packet transmission, confirm the TPID value of the peer device in the public network before adjusting the TPID value.

Configuration Procedure

Follow these steps to adjust the TPID value for VLAN-VPN packets on a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the TPID value globally	**vlan-vpn tpid** *value*	Required Do not set the TPID value to any of the protocol type values listed in Table 1-1. The default TPID value used on the device is 0x8100.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the port to be a VLAN-VPN uplink port	**vlan-vpn uplink enable**	Optional By default, the VLAN-VPN uplink function is disabled.

Caution

- A port cannot be configured as both a VLAN VPN port and a VLAN VPN uplink port at the same time.
- With the TPID being 0x8100, every port can be configured as a VLAN VPN uplink port. However, if the TPID value is not the default value, you need to use the **vlan-vpn uplink enable** command to specify a VLAN VPN uplink port.
- A VLAN VPN uplink port does not remove the outer VLAN tags of packets to be sent through it, so a VLAN VPN uplink port must be configured as a trunk port or hybrid port and configured to keep the outer VLAN when sending packets of the outer VLAN.

Displaying and Maintaining VLAN-VPN

To do…	Use the command…	Remarks
Display the VLAN-VPN configurations of all the ports	**display port vlan-vpn**	Available in any view

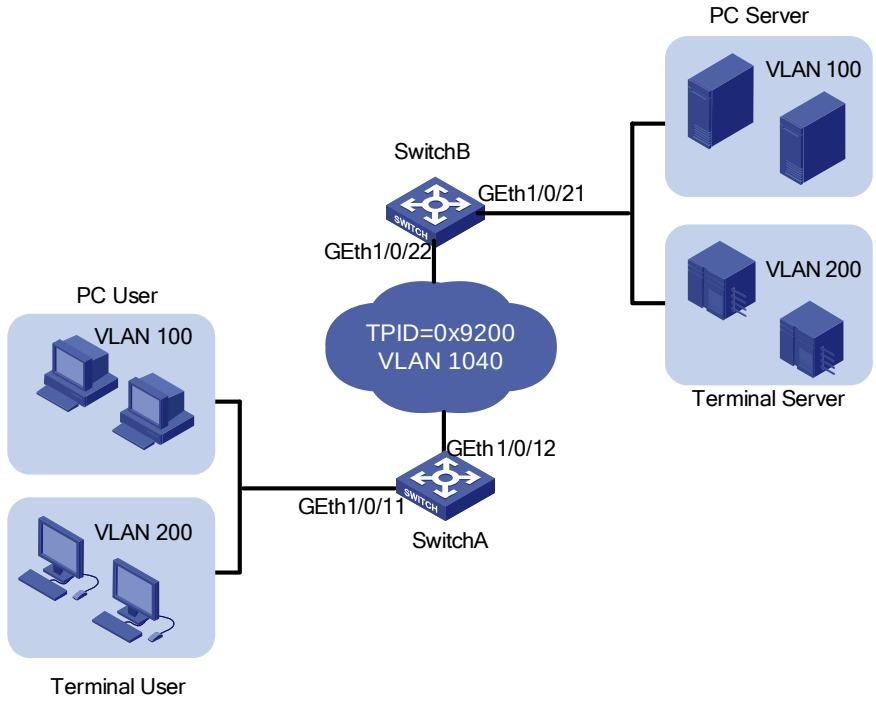
VLAN-VPN Configuration Example

Transmitting User Packets through a Tunnel in the Public Network by Using VLAN-VPN

Network requirements

- As shown in Figure 1-4, both Switch A and Switch B are the WX3000 series devices. They connect the users to the servers through the public network.
- PC users and PC servers are in VLAN 100 created in the private network, while terminal users and terminal servers are in VLAN 200, which is also created in the private network. The VLAN VPN connection is established in VLAN 1040 of the public network.
- Switches of other vendors are used in the public network. They use the TPID value 0x9200.
- Employ VLAN-VPN on Switch A and Switch B to enable the PC users and PC servers to communicate with each through a VPN, and employ VLAN-VPN on Switch A and Switch B to enable the Terminal users and Terminal servers to communicate with each other through a VPN.

Figure 1-4 Network diagram for VLAN-VPN configuration



Configuration procedure

- Configure Switch A.

Enable the VLAN-VPN feature on GigabitEthernet 1/0/11 of Switch A and tag the packets received on this port with the tag of VLAN 1040 as the outer VLAN tag.

```
<SwitchA> system-view
[SwitchA] vlan 1040
[SwitchA-vlan1040] port GigabitEthernet 1/0/11
[SwitchA-vlan1040] quit
[SwitchA] interface GigabitEthernet 1/0/11
[SwitchA-GigabitEthernet1/0/11] vlan-vpn enable
[SwitchA-GigabitEthernet1/0/11] quit
```

Set the global TPID value of Switch A to 0x9200 and configure GigabitEthernet 1/0/12 as a VLAN VPN uplink port, so that Switch A can intercommunicate with devices in the public network.

```
[SwitchA] vlan-vpn tpid 9200
[SwitchA] interface GigabitEthernet1/0/12
[SwitchA-GigabitEthernet1/0/12] port link-type trunk
[SwitchA-GigabitEthernet1/0/12] port trunk permit vlan 1040
[SwitchA-GigabitEthernet1/0/12] vlan-vpn uplink enable
```

- Configure Switch B.

Enable the VLAN-VPN feature on GigabitEthernet 1/0/21 of Switch B and tag the packets received on this port with the tag of VLAN 1040 as the outer VLAN tag.

```
<SwitchB> system-view
[SwitchB] vlan 1040
[SwitchB-vlan1040] port GigabitEthernet 1/0/21
[SwitchB-vlan1040] quit
[SwitchB] interface GigabitEthernet 1/0/21
[SwitchB-GigabitEthernet1/0/21] vlan-vpn enable
```

Set the global TPID value of Switch B to 0x9200 and configure GigabitEthernet 1/0/22 as a VLAN VPN uplink port, so that Switch B can intercommunicate with devices in the public network.

```
[SwitchB-GigabitEthernet1/0/21] quit
[SwitchB] vlan-vpn tpid 9200
[SwitchB] interface GigabitEthernet1/0/22
[SwitchB-GigabitEthernet1/0/22] port link-type trunk
[SwitchB-GigabitEthernet1/0/22] port trunk permit vlan 1040
[SwitchB-GigabitEthernet1/0/22] vlan-vpn uplink enable
```

Note

- Do not configure VLAN 1040 as the default VLAN of GigabitEthernet 1/0/12 of Switch A and GigabitEthernet 1/0/22 of Switch B. Otherwise, the outer VLAN tag of a packet will be removed during transmission.
- In this example, both GigabitEthernet 1/0/11 of Switch A and GigabitEthernet 1/0/21 of Switch B are access ports. In cases where the ports are trunk ports or hybrid ports, you need to configure the two ports to remove the outer VLAN tags before transmitting packets of VLAN 1040. Refer to *Port Basic Configuration* in this manual for detailed configuration.

- Configure the devices in the public network

As the devices in the public network are from other vendors, only the basic principles are introduced here. That is, you need to configure the devices connecting to GigabitEthernet 1/0/12 of Switch A and GigabitEthernet 1/0/22 of Switch B to permit the corresponding ports to transmit tagged packets of VLAN 1040.

Data transfer process

The following describes how a packet is forwarded from Switch A to Switch B in this example.

1) As GigabitEthernet 1/0/11 of Switch A is a VLAN-VPN port, when a packet from the customer's network side reaches this port, it is tagged with the default VLAN tag of the port (VLAN 1040).
2) The device sets the TPID value for the outer VLAN tags of packets to user-defined value 0x9200 and then forwards these packets to the public network through the VLAN-VPN uplink port GigabitEthernet 1/0/12.
3) The outer VLAN tag of the packet remains unchanged while the packet travels in the public network, till it reaches GigabitEthernet 1/0/22 of Switch B.
4) After the packet reaches Switch B, it is forwarded to GigabitEthernet 1/0/21 of Switch B. As the port belongs to VLAN 1040 and is an access port, the outer VLAN tag (the tag of VLAN 1040) of the packet is removed before the packet is forwarded, which restores the packet to a packet tagged with only the private VLAN tag and enables it to be forwarded to its destination networks.
5) It is the same case when a packet travels from Switch B to Switch A.

2 Selective QinQ Configuration

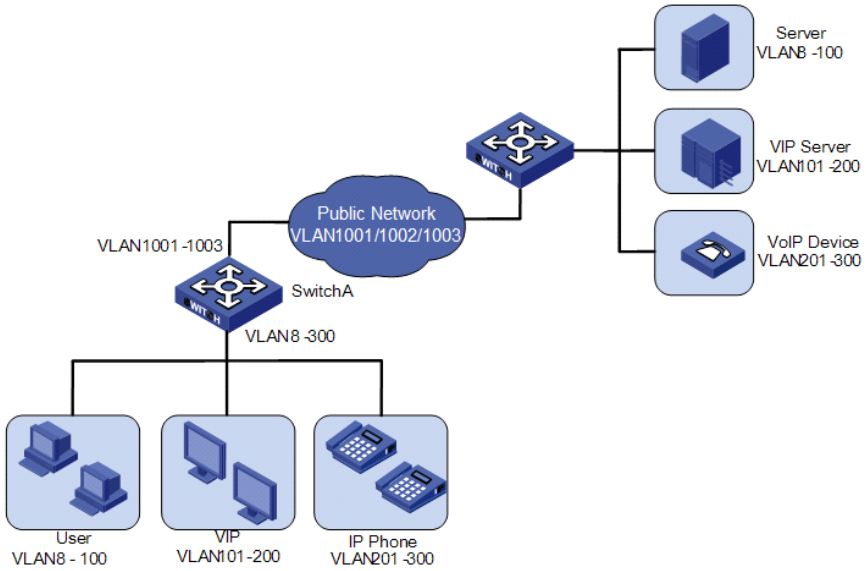
Selective QinQ Overview

Selective QinQ Overview

Selective QinQ is an enhanced application of the VLAN-VPN feature. With the selective QinQ feature, you can configure inner-to-outer VLAN tag mapping, according to which you can add different outer VLAN tags to the packets with different inner VLAN tags.

The selective QinQ feature makes the service provider network structure more flexible. You can classify the terminal users on the port connecting to the access layer device according to their VLAN tags, and add different outer VLAN tags to these users. In the public network, you can configure QoS policies based on outer VLAN tags to assign different priorities to different packets, thus providing differentiated services. See Figure 2-1 for details.

Figure 2-1 Diagram for a selective QinQ implementation



In this implementation, Switch A is an access device of the service provider. The users connecting to it include common customers (in VLAN 8 to VLAN 100), VIPs (in VLAN 101 to VLAN 200), and IP telephone users (in VLAN 201 to VLAN 300). Packets of all these users are forwarded by Switch A to the public network.

After the selective QinQ feature and the inner-to-outer tag mapping feature are enabled on the port connecting Switch A to these users, the port will add different outer VLAN tags to the packets according to their inner VLAN tags. For example, you can configure to add the tag of VLAN 1002 to the packets of IP telephone users in VLAN 201 to VLAN 300 and forward the packets to the VoIP device, which is responsible for processing IP telephone services.

To guarantee the quality of voice packet transmission, you can configure QoS policies in the public network to reserve bandwidth for packets of VLAN 1002 and forward them preferentially.

In this way, you can configure different forwarding policies for data of different type of users, thus improving the flexibility of network management. On the other hand, network resources are well utilized, and users of the same type are also isolated by their inner VLAN tags. This helps to improve network security.

Inner-to-Outer Tag Priority Mapping

As shown in Figure 1-3, the user priority field is the 802.1p priority of the tag. The value of this 3-bit field is in the range 0 to 7. By configuring inner-to-outer tag priority mapping for a VLAN-VPN-enabled port, you can assign outer tags of different priorities to packets according to their inner tag priorities.

Refer to *QoS-QoS profile* part for information about priority.

Selective QinQ Configuration

Configuration Task List

Complete the following tasks to configure selective QinQ:

Task	Remarks
Enabling the Selective QinQ Feature for a Port	Required
Configuring the Inner-to-Outer Tag Priority Mapping Feature	Optional

Enabling the Selective QinQ Feature for a Port

The following configurations are required for the selective QinQ feature:

- Enabling the VLAN-VPN feature on the current port
- Configuring the current port to permit packets of specific VLANs (the VLANs whose tags are to be used as the outer VLAN tags are required)

Follow these steps to enable the selective QinQ feature:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the outer VLAN tag and enter QinQ view	**vlan-vpn vid** *vlan-id*	Required
Configure to add outer VLAN tags to the packets with the specific inner VLAN tags	**raw-vlan-id inbound** *vlan-id-list*	Required By default, the feature of adding an outer VLAN tag to the packets with the specific inner VLAN tags is disabled.

Note

You are recommended not to configure both the DHCP snooping and selective Q-in-Q function on the device, which may result in the DHCP snooping to function abnormally.

Configuring the Inner-to-Outer Tag Priority Mapping Feature

Configuration Prerequisites

Enabling the VLAN-VPN feature on the current port

Configuration Procedure

Follow these steps to configure the inner-to-outer tag priority mapping feature:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the inner-to-outer tag priority mapping feature and create a priority mapping	**vlan-vpn priority** *old-priority* **remark** *new-priority*	Required By default, the inner-to-outer tag priority mapping feature is not enabled.

Selective QinQ Configuration Example

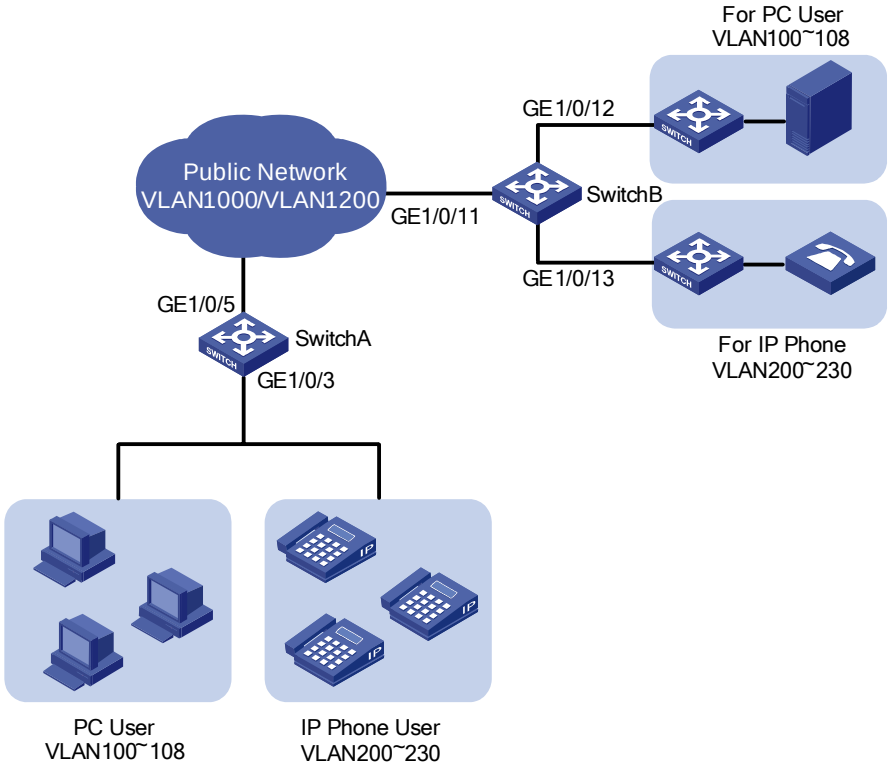
Processing Private Network Packets by Their Types

Network requirements

As shown in Figure 2-2:

- GigabitEthernet 1/0/3 of Switch A provides public network access for PC users and IP phone users. PC users belong to VLAN 100 through VLAN 108, and IP phone users belong to VLAN 200 through VLAN 230. GigabitEthernet 1/0/5 of Switch A is connected to the public network. The peer end of Switch A is Switch B.
- GigabitEthernet 1/0/11 of Switch B is connected to the public network. GigabitEthernet 1/0/12 and GigabitEthernet 1/0/13 of Switch B provide network access for PC servers belonging to VLAN 100 through VLAN 108 and voice gateways (for IP phone users) belonging to VLAN 200 through VLAN 230 respectively.
- The public network permits packets of VLAN 1000 and VLAN 1200. Apply QoS policies for these packets to reserve bandwidth for packets of VLAN 1200. That is, packets of VLAN 1200 have higher transmission priority over packets of VLAN 1000.
- Employ the selective QinQ feature on Switch A and Switch B to differentiate traffic of PC users from that of IP phone users, for the purpose of using QoS policies to guarantee higher priority for voice traffic.
- To reduce broadcast packets in the network, enable the inter-VLAN MAC address replicating feature for selective QinQ.

Figure 2-2 Network diagram for selective QinQ configuration



Configuration procedure

- Configure Switch A.

Create VLAN 1000, VLAN 1200 and VLAN 5 (the default VLAN of GigabitEthernet 1/0/3) on SwitchA.

```
<SwitchA> system-view
[SwitchA] vlan 1000
[SwitchA-vlan1000] quit
[SwitchA] vlan 1200
[SwitchA-vlan1200] quit
[SwitchA] vlan 5
[SwitchA-vlan5] quit
```

Configure GigabitEthernet 1/0/5 as a hybrid port and configure VLAN 5 as its default VLAN. Configure GigabitEthernet 1/0/5 not to remove VLAN tags when forwarding packets of VLAN 5, VLAN 1000, and VLAN 1200.

```
[SwitchA] interface GigabitEthernet 1/0/5
[SwitchA-GigabitEthernet1/0/5] port link-type hybrid
[SwitchA-GigabitEthernet1/0/5] port hybrid pvid vlan 5
[SwitchA-GigabitEthernet1/0/5] port hybrid vlan 5 1000 1200 tagged
[SwitchA-GigabitEthernet1/0/5] quit
```

Configure GigabitEthernet 1/0/3 as a hybrid port and configure GigabitEthernet 1/0/3 to remove VLAN tags when forwarding packets of VLAN 5, VLAN 1000, and VLAN 1200.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type hybrid
[SwitchA-GigabitEthernet1/0/3] port hybrid vlan 5 1000 1200 untagged
```

Enable the VLAN-VPN feature on GigabitEthernet 1/0/3.

```
[SwitchA-GigabitEthernet1/0/3] vlan-vpn enable
```

Enable the selective QinQ feature on GigabitEthernet 1/0/3 to tag packets of VLAN 100 through VLAN 108 with the tag of VLAN 1000 as the outer VLAN tag, and tag packets of VLAN 200 through VLAN 230 with the tag of VLAN 1200 as the outer VLAN tag.

```
[SwitchA-GigabitEthernet1/0/3] vlan-vpn vid 1000
[SwitchA-GigabitEthernet1/0/3-vid-1000] raw-vlan-id inbound 100 to 108
[SwitchA-GigabitEthernet1/0/3-vid-1000] quit
[SwitchA-GigabitEthernet1/0/3] vlan-vpn vid 1200
[SwitchA-GigabitEthernet1/0/3-vid-1200] raw-vlan-id inbound 200 to 230
```

After the above configuration, packets of VLAN 100 through VLAN 108 (that is, packets of PC users) are tagged with the tag of VLAN 1000 as the outer VLAN tag when they are forwarded to the public network by Switch A; and packets of VLAN 200 through VLAN 230 (that is, packets of IP phone users) are tagged with the tag of VLAN 1200 as the outer VLAN tag when they are forwarded to the public network.

- Configure Switch B.

Create VLAN 1000, VLAN 1200, VLAN 12 (the default VLAN of GigabitEthernet 1/0/12) and VLAN 13 (the default VLAN of GigabitEthernet 1/0/13) on Switch B.

```
<SwitchB> system-view
[SwitchB] vlan 1000
[SwitchB-vlan1000] quit
[SwitchB] vlan 1200
[SwitchB-vlan1200] quit
[SwitchB] vlan 12 to 13
```

Configure GigabitEthernet 1/0/11 as a hybrid port, and configure GigabitEthernet 1/0/11 not to remove VLAN tags when forwarding packets of VLAN 12, VLAN 13, VLAN 1000, and VLAN 1200.

```
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 1/0/11
[SwitchB-GigabitEthernet1/0/11] port link-type hybrid
[SwitchB-GigabitEthernet1/0/11] port hybrid vlan 12 13 1000 1200 tagged
```

Configure GigabitEthernet 1/0/12 as a hybrid port and configure VLAN 12 as its default VLAN. Configure GigabitEthernet 1/0/12 to remove VLAN tags when forwarding packets of VLAN 12 and VLAN 1000.

```
[SwitchB] interface GigabitEthernet 1/0/12
[SwitchB-GigabitEthernet1/0/12] port link-type hybrid
[SwitchB-GigabitEthernet1/0/12] port hybrid pvid  vlan 12
[SwitchB-GigabitEthernet1/0/12] port hybrid vlan 12 1000 untagged
[SwitchB-GigabitEthernet1/0/12] quit
```

Configure GigabitEthernet 1/0/13 as a hybrid port and configure VLAN 13 as its default VLAN . Configure GigabitEthernet 1/0/13 to remove VLAN tags when forwarding packets of VLAN 13 and VLAN 1200.

```
[SwitchB] interface GigabitEthernet 1/0/13
[SwitchB-GigabitEthernet1/0/13] port link-type hybrid
[SwitchB-GigabitEthernet1/0/13] port hybrid pvid vlan 13
[SwitchB-GigabitEthernet1/0/13] port hybrid vlan 13 1200 untagged
```

After the above configuration, Switch B can forward packets of VLAN 1000 and VLAN 1200 to the corresponding servers through GigabitEthernet 1/0/12 and GigabitEthernet 1/0/13 respectively.

To make the packets from the servers be transmitted to the clients in the same way, you need to configure the selective QinQ feature on GigabitEthernet 1/0/12 and GigabitEthernet 1/0/13. The configuration on Switch B is similar to that on Switch A and is thus omitted.

Note

- The port configuration on Switch B is only an example for a specific network requirement. The key to this example is to enable the ports to receive and forward packets of specific VLANs. So you can also configure the ports as access or trunk ports. Refer to *Port Basic Configuration* for details.
- A selective QinQ-enabled device tags a user packet with an outer VLAN tag regardless of the VLAN tag of the user packet, so there is no need to configure user VLANs on the device.
- Make sure the packets of the default VLAN of a selective QinQ-enabled port are permitted on both the local port and the port connecting to the public network.

Table of Contents

1 HWPing Configuration 1-1
HWPing Overview 1-1
Introduction to HWPing 1-1
Test Types Supported by HWPing 1-2
HWPing Test Parameters 1-2
HWPing Configuration 1-4
Configuration on a HWPing Server 1-4
HWPing Client Configuration 1-5
Displaying and Maintaining HWPing 1-17
HWPing Configuration Example 1-17
ICMP Test 1-17
DHCP Test 1-18
FTP Test 1-20
HTTP Test 1-22
Jitter Test 1-23
SNMP Test 1-25
TCP Test (Tcpprivate Test) on the Specified Ports 1-27
UDP Test (Udpprivate Test) on the Specified Ports 1-29
DNS Test 1-30

1 HWPing Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a WX3000.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

HWPing Overview

Introduction to HWPing

HWPing (pronounced Hua'Wei Ping) is a network diagnostic tool. It is used to test the performance of various protocols running in networks. HWPing provides more functions than the **ping** command.

- The **ping** command can only use the ICMP protocol to test the round trip time (RTT) between this end and a specified destination end for the user to judge whether the destination end is reachable.
- Besides the above function of the **ping** command, HWPing can also provide other functions, such as testing the status (open/close) of a DHCP/FTP/HTTP/SNMP server and the response time of various services.

You need to configure HWPing client and sometimes the corresponding HWPing servers as well to perform various HWPing tests.

All HWPing tests are initiated by HWPing client and you can view the test results on HWPing client only.

When performing a HWPing test, you need to configure a HWPing test group on the HWPing client. A HWPing test group is a set of HWPing test parameters. A test group contains several test parameters and is uniquely identified by an administrator name and a test tag.

After creating a HWPing test group and configuring the test parameters, you can then perform a HWPing test by the **test-enable** command.

- Being different from the **ping** command, HWPing does not display the RTT or timeout status of each packet on the Console terminal in real time. To view the statistic results of your HWPing test operation, you need to execute the **display hwping** command.
- HWPing also allows you to set parameters for HWPing test groups, start HWPing tests and view statistical test results through a network management device.

Figure 1-1 HWPing illustration



Test Types Supported by HWPing

Table 1-1 Test types supported by HWPing

Supported test types		Description
ICMP test		For these types of tests, you need to configure HWPing client and corresponding servers.
DHCP test		
FTP test		
HTTP test		
DNS test		
SNMP test		
Jitter test		• These types of tests need the cooperation of HWPing client and HWPing Server. • Do not perform TCP or UDP test on port 1 to 1023 (well-known ports). Otherwise your HWPing test may fail or cause the service corresponding to the well-known port (1 to 1023) being unavailable.
TCP test	Tcppublic test	
	Tcpprivate test	
UDP test	Udppublic test	
	Udpprivate test	

HWPing Test Parameters

You need to configure corresponding test parameters for each type of HWPing test. HWPing test parameters can be configured on HWPing client only. For the configurations on HWPing client, refer to section.

Table 1-2 HWPing test parameters

Test parameter	Description
Destination address (**destination-ip**)	For TCP/UDP/jitter test, you must specify a destination IP address, and the destination address must be the IP address of a TCP/UDP/UDP listening service configured on the HWPing server.
Destination port (**destination-port**)	For tcpprivate/udpprivate/jitter test, you must specify a destination port number, and the destination port number must be the port number of a TCP or UDP listening service configured on the HWPing server.

Test parameter	Description
Source interface (**source-interface**)	• For DHCP test, you must specify a source interface, which will be used by HWPing client to send DHCP requests. If no source interface is specified for a DHCP test, the test will not succeed. • After a source interface is specified, HWPing client uses this source interface to send DHCP requests during a DHCP test. • The IP address of the specified source interface will be used as the source IP address of DHCP requests.
Source address (**source-ip**)	For HWPing tests other than DHCP test, you can specify a source IP address for test packets, which will be used by the server as the destination address of response packets.
Source port (**source-port**)	For HWPing tests other than ICMP, DHCP and DNS, you can specify a source port number for test packets, which will be used by the server as the destination port number of response packets.
Test type (**test-type**)	• You can use HWPing to test a variety of protocols, see Table 1-1 for details. • To perform a type of test, you must first create a test group of this type. One test group can be of only one HWPing test type.
Number of probes per test (**count**)	• For tests except jitter test, only one test packet is sent in a probe. In a jitter test, you can use the **jitter-packetnum** command to set the number of packets to be sent in a probe.
Packet size (**datasize**)	• For ICMP/UDP/jitter test, you can configure the size of test packets. • For ICMP test, the ICMP packet size refers to the length of ECHO-REQUEST packets (excluding IP and ICMP headers)
Maximum number of history records that can be saved (**history-records**)	This parameter is used to specify the maximum number of history records that can be saved in a test group. When the number of saved history records exceeds the maximum number, HWPing discards some earliest records.
Automatic test interval (**frequency**)	This parameter is used to set the interval at which the HWPing client periodically performs the same test automatically.
Probe timeout time (**timeout**)	• The probe timeout timer is started after the HWPing client sends out a test packet. • This parameter is in seconds.
Type of service (**tos**)	Type of service is the value of the ToS field in IP header in the test packets.
dns	This parameter is used to specify a DNS domain name in a HWPing DNS test group.
dns-server	This parameter is used to set the DNS server IP address in a HWPing DNS test group.
HTTP operation type (**http-operation**)	This parameter is used to set the type of HTTP interaction operation between HWPing client and HTTP server.
FTP operation type (**ftp-operation**)	This parameter is used to set the type of FTP interaction operation between HWPing client and FTP server.
FTP login username and password (**username** and **password**)	The two parameters are used to set the username and password to be used for FTP operation.

Test parameter	Description
File name for FTP operation (**filename**)	Name of a file to be transferred between HWPing client and FTP server
Number of jitter test packets to be sent per probe (**jitter-packetnum**)	• Jitter test is used to collect statistics about delay jitter in UDP packet transmission • In a jitter probe, the HWPing client sends a series of packets to the HWPing server at regular intervals (you can set the interval). Once receiving such a packet, the HWPing server marks it with a timestamp, and then sends it back to the HWPing client. Upon receiving a packet returned, the HWPing client computes the delay jitter time. The HWPing client collects delay jitter statistics on all the packets returned in the test. So, the more packets a jitter probe sends, the more accurate the jitter statistics is, but the longer time the jitter test costs.
Interval to send jitter test packets (**jitter-interval**)	Each jitter probe will send multiple UDP test packets at regular intervals (you can set the interval). The smaller the interval is, the faster the test is. But a too small interval may somewhat impact your network.
Trap	• A HWPing test will generate a Trap message no matter whether the test successes or not. You can use the Trap device to enable or disable the output of trap messages. • You can set the number of consecutive failed HWPing tests before Trap output. You can also set the number of consecutive failed HWPing probes before Trap output.

HWPing Configuration

The TCP/UDP/jitter tests need the cooperation of HWPing client and HWPing Server, Other types of tests need to configure HWPing client and corresponding different servers.

Configuration on a HWPing Server

You can enable both the HWPing client and HWPing server functions on a device, that is, the device can serve as a HWPing client and server simultaneously.

HWPing server configuration tasks

Complete the following tasks to configure the HWPing server:

Task		Remarks
HWPing server configuration	Enable the HWPing server function	The HWPing server function is needed only for jitter, TCP, and UDP tests.
	Configure a listening service on the HWPing server	You can configure multiple TCP/UDP listening services on one HWPing server, with each listening service corresponding to a specific destination IP address and port number.

HWPing server configuration

The following table describes the configuration on HWPing server, which is the same for HWPing test types that need to configure HWPing server.

Follow these steps to configure the HWPing server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the HWPing server function	**hwping-server enable**	Required Disabled by default.
Configure a UDP listening service	**hwping-server udpecho** *ip-address port-num*	Required for UDP and jitter tests By default, no UDP listening service is configured.
Configure a TCP listening service	**hwping-server tcpconnect** *ip-address port-num*	Required for TCP tests By default, no TCP listening service is configured.

HWPing Client Configuration

HWPing client configuration

After HWPing client is enabled, you can create multiple test groups for different tests, without the need to enable HWPing client repeatedly for each test group.

Different types of HWPing tests are somewhat different in parameters and parameter ranges. The following text describes the configuration on HWPing client for different test types.

1) Configuring ICMP test on HWPing client

Follow these steps to configure ICMP test on HWPing client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the HWPing client function	**hwping-agent enable**	Required By default, the HWPing client function is disabled.
Create a HWPing test group and enter its view	**hwping** *administrator-name operation-tag*	Required By default, no test group is configured.
Configure the destination IP address	**destination-ip** *ip-address*	Required By default, no destination address is configured.
Configure the source IP address	**source-ip** *ip-address*	Optional By default, no source IP address is configured.
Configure the test type	**test-type icmp**	Optional By default, the test type is ICMP.

To do…	Use the command…	Remarks
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.
Configure the packet size	**datasize** *size*	Optional By default, the packet size is 56 bytes.
Configure the maximum number of history records that can be saved	**history-records** *number*	Optional By default, the maximum number is 50.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the type of service (ToS)	**tos** *value*	Optional By default, the service type is zero.
Start the test	**test-enable**	Required
Display test results	**display hwping results** [*admin-name operation-tag*]	Required Available in any view.

Note

For ICMP tests, if no IP address is configured for the specified source interface, the ICMP test will fail; if a source IP address has been configured with the **source-ip** command, the **source-interface** command cannot change the configured IP address.

2) Configuring DHCP test on HWPing client

Follow these steps to configure DHCP test on HWPing client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the HWPing client function	**hwping-agent enable**	Required By default, the HWPing client function is disabled.
Create a HWPing test group and enter its view	**hwping** *administrator-name operation-tag*	Required By default, no test group is configured.

To do…	Use the command…	Remarks
Configure the source interface	**source-interface** *interface-type interface-number*	Required You can only configure a VLAN interface as the source interface. By default, no source interface is configured.
Configure the test type	**test-type dhcp**	Required By default, the test type is ICMP.
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	**history-records** *number*	Optional By default, the maximum number is 50.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Start the test	**test-enable**	Required
Display test results	**display hwping results** [*admin-name operation-tag*]	Required You can execute the command in any view.

3) Configuring FTP test on HWPing client

Follow these steps to configure FTP test on HWPing client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the HWPing client function	**hwping-agent enable**	Required By default, the HWPing client function is disabled.
Create a HWPing test group and enter its view	**hwping** *administrator-name operation-tag*	Required By default, no test group is configured.
Configure the destination IP address	**destination-ip** *ip-address*	Required By default, no destination address is configured.
Configure the source IP address	**source-ip** *ip-address*	Required By default, no source IP address is configured.
Configure the source port	**source-port** *port-number*	Optional By default, no source port is configured.
Configure the test type	**test-type ftp**	Required By default, the test type is ICMP.

To do…	Use the command…	Remarks
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	**history-records** *number*	Optional By default, the maximum number is 50.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the type of service	**tos** *value*	Optional By default, the service type is zero.
Configure the type of FTP operation	**ftp-operation** { **get** | **put** }	Optional By default, the type of FTP operation is **get**, that is, the FTP operation will get a file from the FTP server.
Configure an FTP login username	**username** *name*	Required By default, neither username nor password is configured.
Configure an FTP login password	**password** *password*	
Configure a file name for the FTP operation	**filename** *file-name*	Required By default, no file name is configured for the FTP operation
Start the test	**test-enable**	Required
Display test results	**display hwping results** [*admin-name operation-tag*]	Required You can execute the command in any view.

4) Configuring HTTP test on HWPing client

Follow these steps to configure HTTP test on HWPing client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the HWPing client function	**hwping-agent enable**	Required By default, the HWPing client function is disabled.
Create a HWPing test group and enter its view	**hwping** *administrator-name operation-tag*	Required By default, no test group is configured.

To do…	Use the command…	Remarks
Configure the destination IP address	**destination-ip** *ip-address*	Required You can configure an IP address or a host name. By default, no destination address is configured.
Configure dns-server	**dns-server** *ip-address*	Required when you use the **destination-ip** command to configure the destination address as the host name. By default, no IP address of the DNS server is configured.
Configure the source IP address	**source-ip** *ip-address*	Optional By default, no source IP address is configured.
Configure the source port	**source-port** port-number	Optional By default, no source port is configured.
Configure the test type	**test-type http**	Required By default, the test type is ICMP.
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	**history-records** *number*	Optional By default, the maximum number is 50.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the type of service	**tos** *value*	Optional By default, the service type is zero.
Configure the type of HTTP operation	**http-operation** { **get** | **post** }	Optional By default, the type of HTTP operation is **get**, that is, the HTTP operation will get data from the HTTP server.
Start the test	**test-enable**	Required
Display test results	**display hwping results** [*admin-name operation-tag*]	Required You can execute the command in any view.

5) Configuring jitter test on HWPing client

Follow these steps to configure jitter test on HWPing client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the HWPing client function	**hwping-agent enable**	Required By default, the HWPing client function is disabled.
Create a HWPing test group and enter its view	**hwping** *administrator-name operation-tag*	Required By default, no test group is configured.
Configure the destination IP address	**destination-ip** *ip-address*	Required The destination address must be the IP address of a UDP listening service on the HWPing server. By default, no destination address is configured.
Configure the destination port	**destination-port** *Port-number*	Required The destination port must be the port of a UDP listening service on the HWPing server. By default, no destination port is configured.
Configure the source IP address	**source-ip** *ip-address*	Optional By default, no source IP address is configured.
Configure the source port	**source-port** *port-number*	Optional By default, no source port is configured.
Configure the test type	**test-type jitter**	Required By default, the test type is ICMP.
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	**history-records** *number*	Optional By default, the maximum number is 50.
Configure the packet size	**datasize** *size*	Optional By default, the packet size is 68 bytes.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.

To do…	Use the command…	Remarks
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the type of service	**tos** *value*	Optional By default, the service type is zero.
Configure the number of test packets that will be sent in each jitter probe	**jitter-packetnum** *number*	Optional By default, each jitter probe will send 10 packets.
Configure the interval to send test packets in the jitter test	**jitter-interval** *interval*	Optional By default, the interval is 20 milliseconds.
Start the test	**test-enable**	Required
Display test results	**display hwping results** [*admin-name operation-tag*]	Required You can execute the command in any view.

6) Configuring SNMP test on HWPing client

Follow these steps to configure SNMP test on HWPing client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the HWPing client function	**hwping-agent enable**	Required By default, the HWPing client function is disabled.
Create a HWPing test group and enter its view	**hwping** *administrator-name operation-tag*	Required By default, no test group is configured.
Configure the destination IP address	**destination-ip** *ip-address*	Required By default, no destination address is configured.
Configure the source IP address	**source-ip** *ip-address*	Optional By default, no source IP address is configured.
Configure the source port	**source-port** port-number	Optional By default, no source port is configured.
Configure the test type	**test-type snmpquery**	Required By default, the test type is ICMP.
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.

To do…	Use the command…	Remarks
Configure the maximum number of history records that can be saved	**history-records** *number*	Optional By default, the maximum number is 50.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the type of service	**tos** *value*	Optional By default, the service type is zero.
Start the test	**test-enable**	Required
Display test results	**display hwping results** [*admin-name operation-tag*]	Required You can execute the command in any view.

7) Configuring TCP test on HWPing client

Follow these steps to configure TCP test on HWPing client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the HWPing client function	**hwping-agent enable**	Required By default, the HWPing client function is disabled.
Create a HWPing test group and enter its view	**hwping** *administrator-name operation- tag*	Required By default, no test group is configured.
Configure the destination address	**destination-ip** *ip-address*	Required This IP address and the one configured on the HWPing server for listening services must be the same. By default, no destination address is configured.

To do…	Use the command…	Remarks
Configure the destination port	**destination-port** *port-number*	Required in a Tcpprivate test A Tcppublic test is a TCP connection test on port 7. Use the **hwping-server tcpconnect** *ip-address* 7 command on the server to configure the listening service port; otherwise the test will fail. No port number needs to be configured on the client; any destination port number configured on the client will not take effect. By default, no destination port number is configured.
Configure the source IP address	**source-ip** *ip-address*	Optional By default, the source IP address is not specified.
Configure the source port	**source-port** *port-number*	Optional By default, no source port is specified.
Configure the test type	**test-type** { **tcpprivate | tcppublic** }	Required By default, the test type is ICMP.
Configure the number of probes per test	**count** *times*	Optional By default, one probe is made per time.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the maximum number of history records that can be saved	**history-records** *number*	Optional By default, the maximum number is 50.
Configure the type of service	**tos** *value*	Optional By default, the service type is zero.
Start the test	**test-enable**	Required
Display test results	**display hwping results** [*admin-name operation-tag*]	Required The **display** command can be executed in any view.

8) Configuring UDP test on HWPing client

Follow these steps to configure UDP test on HWPing client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the HWPing client function	**hwping-agent enable**	Required By default, the HWPing client function is disabled.
Create a HWPing test group and enter its view	**hwping** *administrator-name operation- tag*	Required By default, no test group is configured.
Configure the destination address	**destination-ip** *ip-address*	Required This IP address and the one configured on the HWPing server for listening service must be the same. By default, no destination address is configured.
Configure the destination port	**destination-port** *port-number*	• Required in a Udpprivate test • A Udppublic test is a UDP connection test on port 7. Use the hwping-server udpecho ip-address 7 command on the server to configure the listening service port; otherwise the test will fail. No port number needs to be configured on the client; any destination port number configured on the client will not take effect. • By default, no destination port number is configured.
Configure the source IP address	**source-ip** *ip-address*	Optional By default, no source IP address is configured.
Configure the source port	**source-port** *port-number*	Optional By default, no source port is specified.
Configure the test type	**test-type { udpprivate | udppublic }**	Required By default, the test type is ICMP.
Configure the number of probes per test	**count** *times*	Optional By default, one probe is made per test.
Configure the maximum number of history records that can be saved	**history-records** *number*	Optional By default, the maximum number is 50.
Configure the data packet size	**datasize** *size*	Optional By default, the data packet size is 100 bytes.

To do…	Use the command…	Remarks
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the service type	**tos** *value*	Optional By default, the service type is zero.
Start the test	**test-enable**	Required
Display test results	**display hwping results** [*admin-name operation-tag*]	Required The **display** command can be executed in any view.

9) Configuring DNS test on HWPing client

Follow these steps to configure DNS test on HWPing client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the HWPing client function	**hwping-agent enable**	Required By default, the HWPing client function is disabled.
Create a HWPing test group and enter its view	**hwping** *administrator-name operation- tag*	Required By default, no test group is configured.
Configure the source IP address	**source-ip** *ip-address*	Optional By default, no source IP address is specified.
Configure the test type	**test-type dns**	Required By default, the test type is ICMP.
Configure the number of probes per test	**count** *times*	Optional By default, one probe is made per test.
Configure the maximum number of history records that can be saved	**history-records** *number*	Optional By default, the maximum number is 50.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.

To do…	Use the command…	Remarks
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the type of service	**tos** *value*	Optional By default, the service type is zero.
Configure the domain name to be resolved	**dns resolve-targetdomai** *domainname*	Required By default, the domain name to be resolved by DNS is not specified.
Configure the IP address of the DNS server	**dns-server** *ip-address*	Required By default, no DNS server address is configured.
Start the test	**test-enable**	Required
Display test results	**display hwping results** [*admin-name operation-tag*]	Required The **display** command can be executed in any view.

Configuring HWPing client to send Trap messages

Trap messages are generated regardless of whether the HWPing test succeeds or fails. You can specify whether to output Trap messages by enabling/disabling Trap sending.

Follow these steps to configure the HWPing client to send Trap messages:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the HWPing client function	**hwping-agent enable**	Required By default, the HWPing client function is disabled.
Create a HWPing test group and enter its view	**hwping** *administrator-name operation- tag*	Required By default, no test group is configured.
Enable the HWPing client to send Trap messages	**send-trap** { **all |** { **probefailure | testcomplete | testfailure** }***** }	Required By default, Trap sending is disabled.
Configure the number of consecutive unsuccessful HWPing tests before Trap output	**test-failtimes** *times*	Optional By default, Trap messages are sent each time a test fails.
Configure the number of consecutive unsuccessful HWPing probes before Trap output	**probe-failtimes** *times*	Optional By default, Trap messages are sent each time a probe fails.

Displaying and Maintaining HWPing

To do…	Use the command…	Remarks
Display test history	**display hwping history** [*administrator-name operation-tag*]	Available in any view
Display the results of the latest test	**display hwping results** [*administrator-name operation-tag*]	

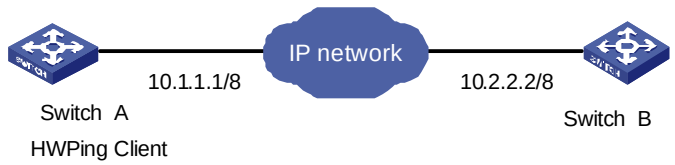
HWPing Configuration Example

ICMP Test

Network requirements

As shown in Figure 1-2, Switch A serves as the HWPing client. A HWPing ICMP test between Switch A and Switch B uses ICMP to test the round trip time (RTT) for packets generated by the HWPing client to travel to and back from the destination.

Figure 1-2 Network diagram for the ICMP test



Configuration procedure

- Configure HWPing Client (Switch A):

Enable HWPing client.

```
<device> system-view
[device] hwping-agent enable
```

Create a HWPing test group, setting the administrator name to "administrator" and test tag to "ICMP".

```
[device] hwping administrator icmp
```

Configure the test type as **icmp**.

```
[device-hwping-administrator-icmp] test-type icmp
```

Configure the destination IP address as 10.2.2.2.

```
[device-hwping-administrator-icmp] destination-ip 10.2.2.2
```

Configure to make 10 probes per test.

```
[device-hwping-administrator-icmp] count 10
```

Set the probe timeout time to 5 seconds.

```
[device-hwping-administrator-icmp] timeout 5
```

Start the test.

```
[device-hwping-administrator-icmp] test-enable
```

Set the maximum number of history records that can be saved to 5.

```
[device-hwping-administrator-icmp] history-records 5
```

Display test results.

```
[device-hwping-administrator-icmp] display hwping results administrator icmp
HWPing entry(admin administrator, tag icmp) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 3/6/3
      Square-Sum of Round Trip Time: 145
      Last succeeded test time: 2000-4-2 20:55:12.3
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[device-hwping-administrator-icmp] display hwping history administrator icmp
HWPing entry(admin administrator, tag icmp) history record:
    Index     Response    Status      LastRC      Time
        1            3         1           0    2000-04-02 20:55:12.3
        2            4         1           0    2000-04-02 20:55:12.3
        3            4         1           0    2000-04-02 20:55:12.2
        4            3         1           0    2000-04-02 20:55:12.2
        5            3         1           0    2000-04-02 20:55:12.2
```

For detailed output description, see the corresponding command manual.

DHCP Test

Network requirements

As shown in Figure 1-3, Switch A serves as a HWPing client and the DHCP server (Switch B) is an H3C S5600 series Ethernet switch. Perform a HWPing DHCP test between the two devices to test the time required for the HWPing client to obtain an IP address from the DHCP server.

Figure 1-3 Network diagram for the DHCP test



Configuration procedure

- Configure DHCP Server(Switch B):

Configure DHCP server on Switch B. For specific configuration of DHCP server, refer to the *DHCP* module.

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<device> system-view
[device] hwping-agent enable
```

Create a HWPing test group, setting the administrator name to "administrator" and test tag to "DHCP".

```
[device] Hwping administrator dhcp
```

Configure the test type as **dhcp**.

```
[device-hwping-administrator-dhcp] test-type dhcp
```

Configure the source interface, which must be a VLAN interface. Make sure the DHCP server resides on the network connected to this interface.

```
[device-hwping-administrator-dhcp] source-interface Vlan-interface 1
```

Configure to make 10 probes per test.

```
[device-hwping-administrator-dhcp] count 10
```

Set the probe timeout time to 5 seconds.

```
[device-hwping-administrator-dhcp] timeout 5
```

Start the test.

```
[device-hwping-administrator-dhcp] test-enable
```

Display test results

```
[device-hwping-administrator-dhcp] display hwping results administrator dhcp
HWPing entry(admin administrator, tag dhcp) test result:
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 1018/1037/1023
      Square-Sum of Round Trip Time: 10465630
      Last complete test time: 2000-4-3 9:51:30.9
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[device-hwping-administrator-dhcp] display hwping history administrator dhcp
HWPing entry(admin administrator, tag dhcp) history record:
    Index     Response    Status      LastRC      Time
        1         1018         1           0    2000-04-03 09:51:30.9
        2         1037         1           0    2000-04-03 09:51:22.9
        3         1024         1           0    2000-04-03 09:51:18.9
        4         1027         1           0    2000-04-03 09:51:06.8
        5         1018         1           0    2000-04-03 09:51:00.8
        6         1020         1           0    2000-04-03 09:50:52.8
        7         1018         1           0    2000-04-03 09:50:48.8
        8         1020         1           0    2000-04-03 09:50:36.8
        9         1020         1           0    2000-04-03 09:50:30.8
       10         1028         1           0    2000-04-03 09:50:22.8
```

For detailed output description, see the corresponding command manual.

FTP Test

Network requirements

As shown in Figure 1-4, both the HWPing client and the FTP server are WX3000 series devices. Perform a HWPing FTP test between the two devices to test the connectivity to the specified FTP server and the time required to upload a file to the server after the connection is established. Both the username and password used to log in to the FTP server are “admin”. The file to be uploaded to the server is cmdtree.txt.

Figure 1-4 Network diagram for the FTP test



Configuration procedure

- Configure FTP Server (Switch B):

Configure FTP server on Switch B. For specific configuration of FTP server, refer to the FTP-SFTP-TFTP part of the manual.

- Configure HWPing Client (Switch A):

Configure the IP address for the Ethernet interface.

```
<device> system-view
[device] interface Vlan-interface 1
[device-Vlan-interface1] ip address 10.1.1.1 8
```

Enable the HWPing client.

```
[device] hwping-agent enable
```

Create a HWPing test group, setting the administrator name to "administrator" and test tag to "FTP".

```
[device] hwping administrator ftp
```

Configure the test type as **ftp**.

```
[device-hwping-administrator-ftp] test-type ftp
```

Configure the IP address of the FTP server as 10.2.2.2.

```
[device-hwping-administrator-ftp] destination-ip 10.2.2.2
```

Configure the FTP login username.

```
[device-hwping-administrator-ftp] username admin
```

Configure the FTP login password.

```
[device-hwping-administrator-ftp] password admin
```

Configure the type of FTP operation.

```
[device-hwping-administrator-ftp] ftp-operation put
```

Configure a file name for the FTP operation.

```
[device-hwping-administrator-ftp] filename cmdtree.txt
```

Configure to make 10 probes per test.

```
[device-hwping-administrator-ftp] count 10
```

Set the probe timeout time to 30 seconds.

```
[device-hwping-administrator-ftp] timeout 30
```

Configure the source IP address

```
[device-hwping-administrator-ftp] source-ip 10.1.1.1
```

Start the test.

```
[device-hwping-administrator-ftp] test-enable
```

Display test results

```
[device-hwping-administrator-ftp] display hwping results administrator ftp
HWPing entry(admin administrator, tag ftp) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 3245/15891/12157
      Square-Sum of Round Trip Time: 1644458573
      Last complete test time: 2000-4-3 4:0:34.6
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[device-hwping-administrator-ftp] display hwping history administrator ftp
HWPing entry(admin administrator, tag ftp) history record:
    Index     Response    Status      LastRC      Time
        1        15822         1           0    2000-04-03 04:00:34.6
        2        15772         1           0    2000-04-03 04:00:18.8
        3         9945         1           0    2000-04-03 04:00:02.9
        4        15891         1           0    2000-04-03 03:59:52.9
        5        15772         1           0    2000-04-03 03:59:37.0
        6        15653         1           0    2000-04-03 03:59:21.2
        7         9792         1           0    2000-04-03 03:59:05.5
        8         9794         1           0    2000-04-03 03:58:55.6
        9         9891         1           0    2000-04-03 03:58:45.8
       10         3245         1           0    2000-04-03 03:58:35.9
```

For detailed output description, see the corresponding command manual.

Note

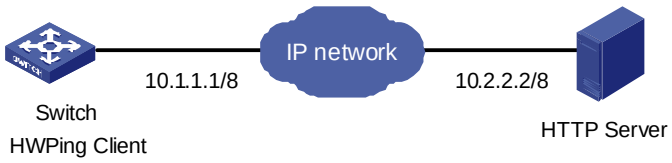
If you are downloading a file from the server, you do not need to specify an FTP operation type. For details, see Configuring FTP test on HWPing client.

HTTP Test

Network requirements

As shown in Figure 1-5, Switch serves as the HWPing client, and a PC serves as the HTTP server. Perform a HWPing HTTP test between Switch and the HTTP server to test the connectivity and the time required to download a file from the HTTP server after the connection to the server is established.

Figure 1-5 Network diagram for the HTTP test



Configuration procedure

- Configure HTTP Server:

Use Windows 2003 Server as the HTTP server. For HTTP server configuration, refer to the related instruction on Windows 2003 Server configuration.

- Configure HWPing Client (Switch):

Enable the HWPing client.

```
<device> system-view
[device] hwping-agent enable
```

Create a HWPing test group, setting the administrator name to "administrator" and test tag to "HTTP".

```
[device] Hwping administrator http
```

Configure the test type as **http**.

```
[device-hwping-administrator-http] test-type http
```

Configure the IP address of the HTTP server as 10.2.2.2.

```
[device-hwping-administrator-http] destination-ip 10.2.2.2
```

Configure to make 10 probes per test.

```
[device-hwping-administrator-http] count 10
```

Set the probe timeout time to 30 seconds.

```
[device-hwping-administrator-http] timeout 30
```

Start the test.

```
[device-hwping-administrator-http] test-enable
```

Display test results

```
[device-hwping-administrator-http] display hwping results administrator http
  HWPing entry(admin administrator, tag http) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 47/87/74
      Square-Sum of Round Trip Time: 57044
      Last succeeded test time: 2000-4-2 20:41:50.4
  Extend result:
```

```
      SD Maximal delay: 0                    DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0         Operation timeout number: 0
      System busy operation number: 0        Connection fail number: 0
      Operation sequence errors: 0           Drop operation number: 0
      Other operation errors: 0
    Http result:
      DNS Resolve Time: 0                  HTTP Operation Time: 675
      DNS Resolve Min Time: 0              HTTP Test Total Time: 748
      DNS Resolve Max Time: 0              HTTP Transmission Successful Times: 10
      DNS Resolve Failed Times: 0          HTTP Transmission Failed Times: 0
      DNS Resolve Timeout Times: 0         HTTP Transmission Timeout Times: 0
      TCP Connect Time: 73                 HTTP Operation Min Time: 27
      TCP Connect Min Time: 5              HTTP Operation Max Time: 80
      TCP Connect Max Time: 20
      TCP Connect Timeout Times: 0
[device-hwping-administrator-http] display hwping history administrator http
HWPing entry(admin administrator, tag http) history record:
    Index     Response    Status      LastRC      Time
       1           13         1           0    2000-04-02 15:15:52.5
       2            9         1           0    2000-04-02 15:15:52.5
       3            3         1           0    2000-04-02 15:15:52.5
       4            3         1           0    2000-04-02 15:15:52.5
       5            3         1           0    2000-04-02 15:15:52.5
       6            2         1           0    2000-04-02 15:15:52.4
       7            3         1           0    2000-04-02 15:15:52.4
       8            3         1           0    2000-04-02 15:15:52.4
       9            2         1           0    2000-04-02 15:15:52.4
      10            2         1           0    2000-04-02 15:15:52.4
```

For detailed output description, see the corresponding command manual.



Note

For an HTTP test, if configuring the destination address as the host name, you must configure the IP address of the DNS server to resolve the host name into an IP address, which is the destination IP address of this HTTP test.

Jitter Test

Network requirements

Both the HWPing client and the HWPing server are WX3000 series devices. Perform a HWPing jitter test between the two devices to test the delay jitter of the UDP packets exchanged between this end (HWPing client) and the specified destination end (HWPing server), with the port number set to 9000.

Network diagram

Figure 1-6 Network diagram for the Jitter test



Configuration procedure

- Configure HWPing Server (Switch B):

Enable the HWPing server and configure the IP address and port to listen on.

```
<device> system-view
[device] hwping-server enable
[device] hwping-server udpecho 10.2.2.2 9000
```

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<device> system-view
[device] hwping-agent enable
```

Create a HWPing test group, setting the administrator name to "administrator" and test tag to "Jitter".

```
[device] hwping administrator Jitter
```

Configure the test type as **jitter**

```
[device-hwping-administrator-Jitter] test-type Jitter
```

Configure the IP address of the HWPing server as 10.2.2.2.

```
[device-hwping-administrator-Jitter] destination-ip 10.2.2.2
```

Configure the destination port on the HWPing server.

```
[device-hwping-administrator-Jitter] destination-port 9000
```

Configure to make 10 probes per test.

```
[device-hwping-administrator-http] count 10
```

Set the probe timeout time to 30 seconds.

```
[device-hwping-administrator-Jitter] timeout 30
```

Start the test.

```
[device-hwping-administrator-Jitter] test-enable
```

Display test results

```
[device-hwping-administrator-Jitter] display hwping results administrator Jitter
HWPing entry(admin administrator, tag Jitter) test result:
      Destination ip address:10.2.2.2
      Send operation times: 100             Receive response times: 100
      Min/Max/Average Round Trip Time: 9/21/13
      Square-Sum of Round Trip Time: 18623
      Last complete test time: 2000-4-2 8:14:58.2
  Extend result:
      SD Maximal delay: 10                  DS Maximal delay: 10
```

```
  Packet lost in test: 0%
  Disconnect operation number: 0        Operation timeout number: 0
  System busy operation number: 0       Connection fail number: 0
  Operation sequence errors: 0          Drop operation number: 0
  Other operation errors: 0
Jitter result:
  RTT Number:100
  Min Positive SD:1                     Min Positive DS:1
  Max Positive SD:6                     Max Positive DS:8
  Positive SD Number:38                 Positive DS Number:25
  Positive SD Sum:85                    Positive DS Sum:42
  Positive SD average:2                 Positive DS average:1
  Positive SD Square Sum:267            Positive DS Square Sum:162
  Min Negative SD:1                     Min Negative DS:1
  Max Negative SD:6                     Max Negative DS:8
  Negative SD Number:30                 Negative DS Number:24
  Negative SD Sum:64                    Negative DS Sum: 41
  Negative SD average:2                 Negative DS average:1
  Negative SD Square Sum:200            Negative DS Square Sum:161
  SD lost packets number:0              DS lost packet number:0
  Unknown result lost packet number:0
[device-hwping-administrator-Jitter] display hwping history administrator Jitter
HWPing entry(admin administrator, tag Jitter) history record:
  Index     Response    Status      LastRC      Time
    1          274         1           0    2000-04-02 08:14:58.2
    2          278         1           0    2000-04-02 08:14:57.9
    3          280         1           0    2000-04-02 08:14:57.6
    4          279         1           0    2000-04-02 08:14:57.3
    5          280         1           0    2000-04-02 08:14:57.1
    6          270         1           0    2000-04-02 08:14:56.8
    7          275         1           0    2000-04-02 08:14:56.5
    8          263         1           0    2000-04-02 08:14:56.2
    9          270         1           0    2000-04-02 08:14:56.0
   10          275         1           0    2000-04-02 08:14:55.7
```

For detailed output description, see the corresponding command manual.

SNMP Test

Network requirements

Both the HWPing client and the SNMP Agent are WX3000 series devices. Perform HWPing SNMP tests between the two devices to test the time required from Switch A sends an SNMP query message to Switch B (SNMP Agent) to it receives a response from Switch B.

Network diagram

Figure 1-7 Network diagram for the SNMP test



Configuration procedure

- Configure SNMP Agent (Switch B):

Start SNMP agent and set SNMP version to V2C, read-only community name to "public", and read-write community name to "private".

```
<Sysname> system-view
[Sysname] snmp-agent
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
```

Note

- The SNMP network management function must be enabled on SNMP agent before it can receive response packets.
- The SNMPv2c version is used as reference in this example. This configuration may differ if the system uses any other version of SNMP. For details, see *SNMP – RMON Operation Manual*.

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<device> system-view
[device] hwping-agent enable
```

Create a HWPing test group, setting the administrator name to "administrator" and test tag to "snmp".

```
[device] Hwping administrator snmp
```

Configure the test type as **snmp**.

```
[device-hwping-administrator-snmp] test-type snmpquery
```

Configure the destination IP address as 10.2.2.2.

```
[device-hwping-administrator-snmp] destination-ip 10.2.2.2
```

Configure to make 10 probes per test.

```
[device-hwping-administrator-snmp] count 10
```

Set the probe timeout time to 30 seconds.

```
[device-hwping-administrator-snmp] timeout 30
```

Start the test.

```
[device-hwping-administrator-snmp] test-enable
```

Display test results

```
[device-hwping-administrator-snmp] display hwping results administrator snmp
HWPing entry(admin administrator, tag snmp) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 9/11/10
      Square-Sum of Round Trip Time: 983
      Last complete test time: 2000-4-3 8:57:20.0
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[device-hwping-administrator-snmp] display hwping history administrator snmp
HWPing entry(admin administrator, tag snmp) history record:
    Index     Response    Status      LastRC      Time
       1           10         1           0    2000-04-03 08:57:20.0
       2           10         1           0    2000-04-03 08:57:20.0
       3           10         1           0    2000-04-03 08:57:20.0
       4           10         1           0    2000-04-03 08:57:19.9
       5            9         1           0    2000-04-03 08:57:19.9
       6           11         1           0    2000-04-03 08:57:19.9
       7           10         1           0    2000-04-03 08:57:19.9
       8           10         1           0    2000-04-03 08:57:19.9
       9           10         1           0    2000-04-03 08:57:19.8
      10           10         1           0    2000-04-03 08:57:19.8
```

For detailed output description, see the corresponding command manual.

TCP Test (Tcpprivate Test) on the Specified Ports

Network requirements

Both the HWPing client and the HWPing server are WX3000 series devices. Perform a HWPing Tcpprivate test to test time required to establish a TCP connection between this end (Switch A) and the specified destination end (Switch B), with the port number set to 8000.

Network diagram

Figure 1-8 Network diagram for the Tcpprivate test



Configuration procedure

- Configure HWPing Server (Switch B):

Enable the HWPing server and configure the IP address and port to listen on.

```
<device> system-view
[device] hwping-server enable
[device] hwping-server tcpconnect 10.2.2.2 8000
```

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<device> system-view
[device] hwping-agent enable
```

Create a HWPing test group, setting the administrator name to "administrator" and test tag to "tcpprivate".

```
[device] Hwping administrator tcpprivate
```

Configure the test type as **tcpprivate**.

```
[device-hwping-administrator-tcpprivate] test-type tcpprivate
```

Configure the IP address of the HWPing server as 10.2.2.2.

```
[device-hwping-administrator-tcpprivate] destination-ip 10.2.2.2
```

Configure the destination port on the HWPing server.

```
[device-hwping-administrator-tcpprivate] destination-port 8000
```

Configure to make 10 probes per test.

```
[device-hwping-administrator-tcpprivate] count 10
```

Set the probe timeout time to 5 seconds.

```
[device-hwping-administrator-tcpprivate] timeout 5
```

Start the test.

```
[device-hwping-administrator-tcpprivate] test-enable
```

Display test results.

```
[device-hwping-administrator-tcpprivate] display hwping results administrator tcpprivate
HWPing entry(admin administrator, tag tcpprivate) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 4/7/5
      Square-Sum of Round Trip Time: 282
      Last complete test time: 2000-4-2 8:26:2.9
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[device-hwping-administrator-tcpprivate] display hwping history administrator tcpprivate
HWPing entry(admin administrator, tag tcpprivate) history record:
```

```
Index      Response     Status       LastRC       Time
    1             4          1            0     2000-04-02 08:26:02.9
    2             5          1            0     2000-04-02 08:26:02.8
    3             4          1            0     2000-04-02 08:26:02.8
    4             5          1            0     2000-04-02 08:26:02.7
    5             4          1            0     2000-04-02 08:26:02.7
    6             5          1            0     2000-04-02 08:26:02.6
    7             6          1            0     2000-04-02 08:26:02.6
    8             7          1            0     2000-04-02 08:26:02.5
    9             5          1            0     2000-04-02 08:26:02.5
   10             7          1            0     2000-04-02 08:26:02.4
```

For detailed output description, see the corresponding command manual.

UDP Test (Udpprivate Test) on the Specified Ports

Network requirements

Both the HWPing client and the HWPing server are WX3000 series devices. Perform a HWPing Udpprivate test on the specified ports between the two devices to test the RTT of UDP packets between this end (HWPing client) and the specified destination end (HWPing server), with the port number set to 8000.

Network diagram

Figure 1-9 Network diagram for the Udpprivate test



Configuration procedure

- Configure HWPing Server (Switch B):

Enable the HWPing server and configure the IP address and port to listen on.

```
<device> system-view
[device] hwping-server enable
[device] hwping-server udpecho 10.2.2.2 8000
```

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<device> system-view
[device] hwping-agent enable
```

Create a HWPing test group, setting the administrator name to "administrator" and test tag to "udpprivate".

```
[device] Hwping administrator udpprivate
```

Configure the test type as **udpprivate**.

```
[device-hwping-administrator-udpprivate] test-type udpprivate
```

Configure the IP address of the HWPing server as 10.2.2.2.

```
[device-hwping-administrator-udpprivate] destination-ip 10.2.2.2
```

Configure the destination port on the HWPing server.

```
[device-hwping-administrator-udpprivate] destination-port 8000
```

Configure to make 10 probes per test.

```
[device-hwping-administrator-udpprivate] count 10
```

Set the probe timeout time to 5 seconds.

```
[device-hwping-administrator-udpprivate] timeout 5
```

Start the test.

```
[device-hwping-administrator-udpprivate] test-enable
```

Display test results.

```
[device-hwping-administrator-udpprivate] display hwping results administrator udpprivate
HWPing entry(admin administrator, tag udpprivate) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 10/12/10
      Square-Sum of Round Trip Time: 1170
      Last complete test time: 2000-4-2 8:29:45.5
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[device-hwping-administrator-udpprivate] display hwping history administrator udpprivate
HWPing entry(admin administrator, tag udpprivate) history record:
    Index     Response    Status      LastRC      Time
       1           11         1           0    2000-04-02 08:29:45.5
       2           12         1           0    2000-04-02 08:29:45.4
       3           11         1           0    2000-04-02 08:29:45.4
       4           11         1           0    2000-04-02 08:29:45.4
       5           11         1           0    2000-04-02 08:29:45.4
       6           11         1           0    2000-04-02 08:29:45.4
       7           10         1           0    2000-04-02 08:29:45.3
       8           10         1           0    2000-04-02 08:29:45.3
       9           10         1           0    2000-04-02 08:29:45.3
      10           11         1           0    2000-04-02 08:29:45.3
```

For detailed output description, see the corresponding command manual.

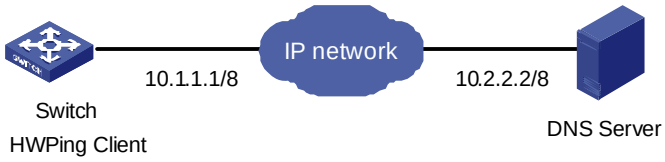
DNS Test

Network requirements

Switch serves as the HWPing client, and a PC serves as the DNS server. Perform a HWPing DNS test between Switch and the DNS server to test the time required from the client sends a DNS request to it receives a resolution result from the DNS server.

Network diagram

Figure 1-10 Network diagram for the DNS test



Configuration procedure

- Configure DNS Server:

Use Windows 2003 Server as the DNS server. For DNS server configuration, refer to the related instruction on Windows 2003 Server configuration.

- Configure HWPing Client (Switch)

Enable the HWPing client.

```
<device> system-view
[device] hwping-agent enable
```

Create a HWPing test group, setting the administrator name to "administrator" and test tag to "dns".

```
[device] hwping administrator dns
```

Configure the test type as **dns**.

```
[device-hwping-administrator-dns] test-type dns
```

Configure the IP address of the DNS server as 10.2.2.2.

```
[device-hwping-administrator-dns] dns-server 10.2.2.2
```

Configure to resolve the domain name www.test.com.

```
[device-hwping-administrator-dns] dns resolve-target www.test.com
```

Configure to make 10 probes per test.

```
[device-hwping-administrator-dns] count 10
```

Set the probe timeout time to 5 seconds.

```
[device-hwping-administrator-dns] timeout 5
```

Start the test.

```
[device-hwping-administrator-dns] test-enable
```

Display test results.

```
[device-hwping-administrator-dns] display hwping results administrator dns
HWPing entry(admin administrator, tag dns) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 6/10/8
      Square-Sum of Round Trip Time: 756
      Last complete test time: 2006-11-28 11:50:40.9
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
```

```
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
    Dns result:
      DNS Resolve Current Time: 10         DNS Resolve Min Time: 6
      DNS Resolve Times: 10                DNS Resolve Max Time: 10
      DNS Resolve Timeout Times: 0         DNS Resolve Failed Times: 0
[device-hwping-administrator-dns] display hwping history administrator dns
HWPing entry(admin administrator, tag dns) history record:
    Index     Response    Status      LastRC      Time
        1           10         1           0    2006-11-28 11:50:40.9
        2           10         1           0    2006-11-28 11:50:40.9
        3           10         1           0    2006-11-28 11:50:40.9
        4            7         1           0    2006-11-28 11:50:40.9
        5            8         1           0    2006-11-28 11:50:40.9
        6            6         1           0    2006-11-28 11:50:40.9
        7            8         1           0    2006-11-28 11:50:40.9
        8            9         1           0    2006-11-28 11:50:40.9
        9            9         1           0    2006-11-28 11:50:40.9
       10            9         1           0    2006-11-28 11:50:40.9
```

For detailed output description, see the corresponding command manual.

Table of Contents

1 DNS Configuration 1-1
DNS Overview 1-1
Static Domain Name Resolution 1-1
Dynamic Domain Name Resolution 1-1
Configuring Domain Name Resolution 1-2
Configuring Static Domain Name Resolution 1-2
Configuring Dynamic Domain Name Resolution 1-3
DNS Configuration Example 1-3
Static Domain Name Resolution Configuration Example 1-3
Dynamic Domain Name Resolution Configuration Example 1-4
Displaying and Maintaining DNS 1-6
Troubleshooting DNS Configuration 1-6

1 DNS Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.
- This chapter covers only IPv4 DNS configuration. For details about IPv6 DNS, refer to *IPv6 Management Operation*.

DNS Overview

Domain name system (DNS) is a mechanism used for TCP/IP applications to provide domain name-to-IP address translation. With DNS, you can use memorizable and meaningful domain names in some applications and let the DNS server resolve it into correct IP addresses.

There are two types of DNS services, static and dynamic. Each time the DNS server receives a name query, it checks its static DNS database before looking up the dynamic DNS database. Reduction of the searching time in the dynamic DNS database would increase efficiency. Some frequently used addresses can be put in the static DNS database.

Static Domain Name Resolution

The static domain name resolution means manually setting up mappings between domain names and IP addresses. IP addresses of the corresponding domain names can be found in the static domain name resolution table for applications, such as Telnet.

Dynamic Domain Name Resolution

Resolution procedure

Dynamic domain name resolution is implemented by querying the DNS server. The resolution procedure is as follows:

1) A user program sends a name query to the resolver in the DNS client.
2) The DNS resolver looks up the local domain name cache for a match. If a match is found, it sends the corresponding IP address back. If not, it sends the query to the DNS server.
3) The DNS server looks up its DNS database for a match. If no match is found, it sends a query to a higher-level DNS server. This process continues until a result, success or failure, is returned.
4) The DNS client performs the next operation according to the result.

Figure 1-1 Dynamic domain name resolution

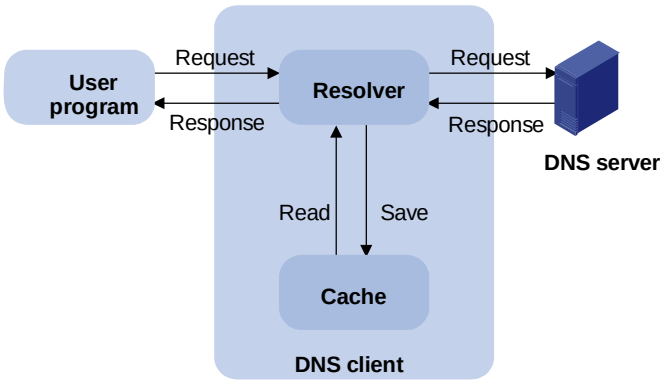


Figure 1-1 shows the relationship between user program, DNS client, and DNS server.

The resolver and cache comprise the DNS client. The user program and DNS client run on the same device, while the DNS server and the DNS client usually run on different devices.

Dynamic domain name resolution allows the DNS client to store latest mappings between name and IP address in the dynamic domain name cache of the DNS client. There is no need to send a request to the DNS server for a repeated query request next time. The aged mappings are removed from the cache after some time, and latest entries are required from the DNS server. The DNS server decides how long a mapping is valid, and the DNS client gets the information from DNS messages.

DNS suffixes

The DNS client normally holds a list of suffixes which can be defined by users. It is used when the name to be resolved is not complete. The resolver can supply the missing part (automatic domain name addition). For example, a user can configure com as the suffix for aabbcc.com. The user only needs to type aabbcc to get the IP address of aabbcc.com. The resolver can add the suffix and delimiter before passing the name to the DNS server.

- If there is no dot in the domain name, such as aabbcc, the resolver will consider this as a host name and add a DNS suffix before processing. The original name such as aabbcc is used if all DNS lookups fail.
- If there is a dot in the domain name, such as www.aabbcc, the resolver will use this domain name to do DNS lookup first. If the lookup fails, the resolver adds a DNS suffix for another lookup.
- If a dot is at the end of the domain name, such as “aabbcc.com.”, the resolver will consider this as a fully qualified domain name and return the result, success or failure. Hence, the dot (.) is called the terminating symbol.

Currently, the device supports both static and dynamic DNS clients.

Configuring Domain Name Resolution

Configuring Static Domain Name Resolution

Follow these steps to configure static domain name resolution:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a mapping between a host name and an IP address	**ip host** *hostname ip-address*	Required No IP address is assigned to a host name by default.

Note

The IP address you assign to a host name last time will overwrite the previous one if there is any.

You may create up to 50 static mappings between domain names and IP addresses.

Configuring Dynamic Domain Name Resolution

Follow these steps to configure dynamic domain name resolution:

To do…	Use the command…	Remarks
Enter the system view	**system-view**	—
Enable dynamic domain name resolution	**dns resolve**	Required Disabled by default
Configure an IP address for the DNS server	**dns server** *ip-address*	Required No IP address is configured for the DNS server by default.
Configure DNS suffixes	**dns domain** *domain-name*	Optional No DNS suffix is configured by default

Note

You may configure up to six DNS servers and ten DNS suffixes.

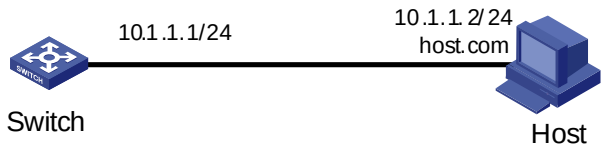
DNS Configuration Example

Static Domain Name Resolution Configuration Example

Network requirements

As shown in Figure 1-2, Switch uses static domain name resolution to access host 10.1.1.2 through domain name host.com.

Figure 1-2 Network diagram for static DNS configuration



Configuration procedure

Configure a mapping between host name host.com and IP address 10.1.1.2.

```
<device> system-view
[device] ip host host.com 10.1.1.2
```

Execute the **ping host.com** command to verify that the device can use static domain name resolution to get the IP address 10.1.1.2 corresponding to host.com.

```
[device] ping host.com
  PING host.com (10.1.1.2): 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=127 time=3 ms
    Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=127 time=3 ms
    Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=127 time=2 ms
    Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=127 time=5 ms
    Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=127 time=3 ms

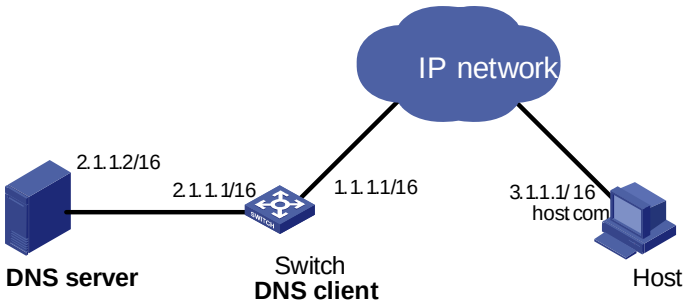

  --- host.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/3/5 ms
```

Dynamic Domain Name Resolution Configuration Example

Network requirements

As shown in Figure 1-3, Switch serving as a DNS client uses dynamic domain name resolution to access the host at 3.1.1.1/16 through its domain name **host**. The DNS server has the IP address 2.1.1.2/16. The DNS suffix is **com**.

Figure 1-3 Network diagram for dynamic DNS configuration



Configuration procedure

Note

Before doing the following configuration, make sure that:

- The routes between the DNS server, Switch, and Host are reachable.
- Necessary configurations are done on the devices. For the IP addresses of the interfaces, see the figure above.
- There is a mapping between domain name **host** and IP address 3.1.1.1/16 on the DNS server.
- The DNS server works normally.

Enable dynamic domain name resolution.

```
<device> system-view
[device] dns resolve
```

Configure the IP address 2.1.1.2 for the DNS server.

```
[device] dns server 2.1.1.2
```

Configure com as the DNS suffix

```
[device] dns domain com
```

Execute the **ping host** command on Switch to verify that the communication between Switch and Host is normal and that the corresponding IP address is 3.1.1.1.

```
[device] ping host
 Trying DNS server (2.1.1.2)
  PING host.com (3.1.1.1): 56  data bytes, press CTRL_C to break
    Reply from 3.1.1.1: bytes=56 Sequence=1 ttl=255 time=3 ms
    Reply from 3.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 3.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/3 ms
  --- host.com ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

Displaying and Maintaining DNS

To do…	Use the command…	Remarks
Display static DNS database	**display ip host**	Available in any view
Display the DNS server information	**display dns server** [**dynamic**]	
Display the DNS suffixes	**display dns domain** [**dynamic**]	
Display the information in the dynamic domain name cache	**display dns dynamic-host**	
Display the DNS resolution result	**nslookup type** { **ptr** *ip-address* | **a** *domain-name* }	Available in any view
Clear the information in the dynamic domain name cache	**reset dns dynamic-host**	Available in user view

Troubleshooting DNS Configuration

Symptom

After enabling the dynamic domain name resolution, the user cannot get the correct IP address.

Solution

- Use the **display dns dynamic-host** command to check that the specified domain name is in the cache.
- If there is no defined domain name, check that dynamic domain name resolution is enabled and the DNS client can communicate with the DNS server.
- If the specified domain name exists in the cache but the IP address is incorrect, check that the DNS client has the correct IP address of the DNS server.
- Check that the mapping between the domain name and IP address is correct on the DNS server.

Table of Contents

1 Smart Link Configuration 1-1
Smart Link Overview 1-1
Basic Concepts in Smart Link 1-1
Operating Mechanism of Smart Link 1-3
Configuring Smart Link 1-3
Configuration Task List 1-3
Configuring a Smart Link Device 1-4
Configuring Associated Devices 1-5
Precautions 1-5
Displaying and Maintaining Smart Link 1-6
Smart Link Configuration Example 1-6
Implementing Link Redundancy Backup 1-6
2 Monitor Link Configuration 2-1
Introduction to Monitor Link 2-1
How Monitor Link Works 2-2
Configuring Monitor Link 2-3
Configuration Task List 2-3
Creating a Monitor Link Group 2-3
Configuring the Uplink Port 2-3
Configuring a Downlink Port 2-4
Displaying and Maintaining Monitor Link 2-5
Monitor Link Configuration Example 2-5
Implementing Collaboration Between Smart Link and Monitor Link 2-5

1 Smart Link Configuration

Note

- The term switch used throughout this chapter refers to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.
- The sample output information in this manual was created on the WX3024. The output information on your device may vary.

Smart Link Overview

As shown in Figure 1-1, dual-uplink networking is widely applied currently. Usually, spanning tree protocol (STP) is used to implement link redundancy backup in the network. However, STP is not suitable for users with a high demand for convergence time. Smart Link can achieve active/standby link redundancy backup and fast convergence to meet the user demand.

Smart Link has the following features:

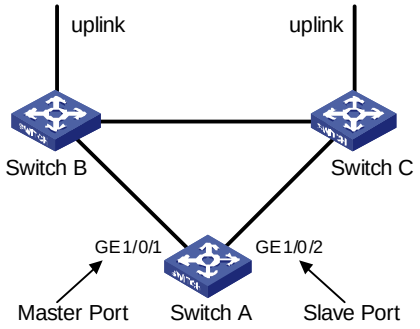
- Active/standby backup for dual-uplink networking
- Simple configuration and operation

Basic Concepts in Smart Link

Smart Link group

A Smart Link group consists of two member ports, one master port and one slave port. Normally, only one port (master or slave) is active, and the other port is blocked, that is, in the standby state. When link failure occurs on the port in active state, the Smart Link group will block the port automatically and turn standby state to active state on the blocked port.

Figure 1-1 Network diagram of Smart Link



In Figure 1-1, GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on Switch A are two member ports of a Smart Link group.

Master port

The master port can be either an Ethernet port or a manually-configured or static LACP aggregation group. For example, you can configure GigabitEthernet 1/0/1 of switch A in Figure 1-1 as the master port through the command line.

Slave port

The slave port can be either an Ethernet port or a manually-configured or static LACP aggregation group. For example, you can configure GigabitEthernet 1/0/2 of switch A in Figure 1-1 as the slave port through the command line.

Flush message

When a forwarding link fails, the device will switch the traffic to the blocked standby link. The former forwarding entries of each device in the network are no longer suitable for the new topology, so MAC address forwarding entries and ARP entries must be updated throughout the network. In this case, the Smart Link group sends flush messages to notify other devices to refresh MAC address forwarding entries and ARP entries.

Control VLAN for sending flush messages

This control VLAN sends flush messages. When link switching occurs, the device (Switch A in Figure 1-1) broadcasts flush messages in this control VLAN.

Control VLAN for receiving flush messages

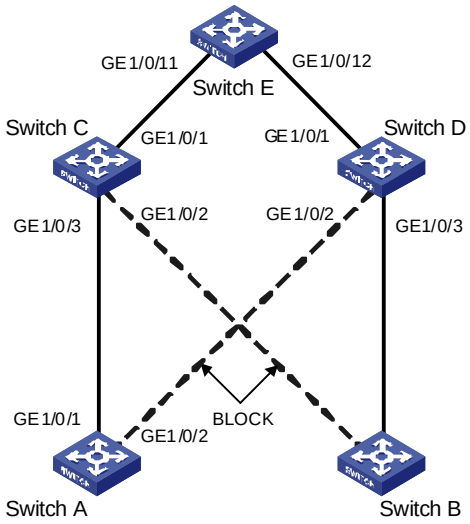
This control VLAN is used for receiving and processing flush messages. When link switching occurs, the devices (Switch B and Switch C in Figure 1-1) receive and process flush messages of this control VLAN, and then refresh MAC forwarding table entries and ARP entries.

Note

- Currently, the member ports of a Smart Link group cannot be dynamic link aggregation groups.
- If the master port or slave port of a Smart Link group is a link aggregation group, you cannot remove this link aggregation group directly or change the aggregation group into a dynamic aggregation group. Before removing this aggregation group, you must unbind the link aggregation group from the Smart Link.

Operating Mechanism of Smart Link

Figure 1-2 Network diagram of Smart Link operating mechanism



As shown in Figure 1-2, GigabitEthernet 1/0/1 on Switch A is active and GigabitEthernet 1/0/2 on Switch A is blocked. When the link connected to GigabitEthernet 1/0/1 fails, GigabitEthernet 1/0/1 is blocked automatically, and the state of GigabitEthernet 1/0/2 turns to active state.

- When link switching occurs in the Smart Link group, MAC forwarding entries and ARP entries of each device in the network may be out of date. In order to guarantee correct packet transmission, you must enable the Smart Link device to send flush messages to notify the other devices in the network to refresh their own MAC forwarding entries and ARP entries. In this case, all the uplink devices must be capable of identifying flush messages from the Smart Link group and refreshing MAC forwarding entries and ARP entries.
- On a Smart Link–enabled device, if a port is blocked due to link failure, the port remains blocked after the link recovers from the failure, and does not preempt the traffic resource. Therefore, the traffic stays stable. The port does not come into the forwarding state until the next link switching.

Configuring Smart Link

Note

Before configuring a member port of a Smart Link group, you must:

- Disable the port to avoid loops, thus preventing broadcast storm.
- Disable STP on the port.

After completing the configuration, you need to enable the Ethernet ports disabled before configuring the Smart Link group.

Configuration Task List

Complete the following tasks to configure Smart Link:

Task		Remarks
Configuring a Smart Link Device	Create a Smart Link group	Required
	Add member ports to the Smart Link group	
	Enable the function of sending flush messages in the specified control VLAN	
Configuring Associated Devices	Enable the function of processing flush messages received from the specified control VLAN	Required

Configuring a Smart Link Device

A Smart Link device refers to a device on which Smart Link is enabled and a Smart Link group is configured, and that sends flush messages from the specified control VLAN. A member port of a Smart Link group can be either an Ethernet port or a manually-configured or static LACP aggregation group. You can configure a port or a link aggregation group as a member of a Smart Link group.

Follow these steps to configure Smart Link (with ports as members of the Smart Link group):

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Create a Smart Link group and enter Smart Link group view		**smart-link group** *group-id*	Required
Enable the function of sending flush messages in the specified control VLAN		**flush enable control-vlan** *vlan-id*	Required By default, no control VLAN for sending flush messages is specified.
Configure a port as a Smart Link group member	Smart Link group view	**port** *interface-type interface-number* { **master** | **slave** }	Required Use either approach
	Ethernet port view	**quit**	
		interface *interface-type interface-number*	
		port smart-link group *group-id* { **master** | **slave** }	

Follow these steps to configure Smart Link (with link aggregation groups are members of the Smart Link group):

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a Smart Link group and enter Smart Link group view	**smart-link group** *group-id*	Required
Configure a link aggregation group as a member of the Smart Link group	**link-aggregation group** *group-id* { **master** | **slave** }	Optional

To do…	Use the command…	Remarks
Enable the function of sending flush messages in the specified control VLAN	**flush enable control-vlan** *vlan-id*	Optional By default, no control VLAN for sending flush messages is specified.

Configuring Associated Devices

An associated device mentioned in this document refers to a device that supports Smart Link and locally configured to process flush messages received from the specified control VLAN so as to work with the corresponding Smart Link device. As shown in Figure 1-2, all the devices including Switch C, Switch D, and Switch E on the active and backup links connecting the Smart Link device (Switch A) and the target uplink device (Switch E) are all associated devices.

However, you do not have to enable all the ports of an associated device to process flush messages received from the specified control VLAN. You need to enable this function only on the ports that are on the active and backup links connecting the Smart Link device and the target device. As shown in Figure 1-2, you need to enable this function on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch C, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch D, and GigabitEthernet 1/0/11 and GigabitEthernet 1/0/12 of Switch E.

Follow these steps to enable the specified port to process flush messages received from the specified control VLAN:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enable the specified port(s) to process flush messages received from the control VLAN	System view	**smart-link flush enable control-vlan** *vlan-id* **port** *interface-type interface-number* [**to** *interface-type interface-number*]	Required, use either approach. By default, no control VLAN for receiving flush messages is specified.
	Ethernet port view	**interface** *interface-type interface-number*	
		smart-link flush enable control-vlan *vlan-id*	

Precautions

When configuring Smart Link, pay attention to the following points:

- A port or a link aggregation group cannot serve as a member port for two Smart Link groups. On the other hand, a port or a link aggregation group cannot serve as a member for a Smart Link group and a Monitor Link group at the same time.
- STP cannot be enabled on the member ports of a Smart Link group. An STP-enabled port or a link aggregation group with an STP-enabled port cannot serve as a member port for a Smart Link group.
- A Smart Link/Monitor Link group with members cannot be deleted.
- Smart Link/Monitor Link is mutually exclusive with remote port mirroring.
- When a Combo port operates as a member port of a Smart Link group, the optical port and the electrical port of the Combo port must not be both engaged with a cable at the same time.

- When you copy a port, the Smart Link/Monitor Link group member information configured on the port will not be copied to other ports.
- If a single port is specified as a member of a Smart Link/Monitor Link group, you cannot execute the **lacp enable** command on this port or add this port into other dynamic link aggregation groups, because these operations will make this port become a link aggregation group member.
- If no control VLAN is configured for flush message processing, the device will forward received flush messages without processing them.
- If the control VLAN for receiving flush messages configured on an associated device is different than the one for sending flush messages configured on the corresponding Smart Link device, the device will forward received flush messages without processing them.
- In the static or manual link aggregation group which serves as a Smart Link group member, if a member port can process flush messages, this function cannot be synchronized to the other ports in the aggregation group automatically, that is, the other member ports in the aggregation group cannot process flush messages. The function of processing flush messages must be manually configured for each port in the aggregation group.
- The VLAN configured as a control VLAN to send and receive flush messages must exist. You cannot directly remove the control VLAN. When a dynamic VLAN is configured as the control VLAN for the Smart Link group, this VLAN will become a static VLAN, and the prompt information is displayed.

Displaying and Maintaining Smart Link

To do…	Use the command…	Remarks
Display the information of a Smart Link group	**display smart-link group** { *group-id* | **all** }	Available in any view
Display the statistics information of flush messages received and processed by the current device	**display smart-link flush**	
Clear flush message statistics	**reset smart-link packets counter**	Available in any view

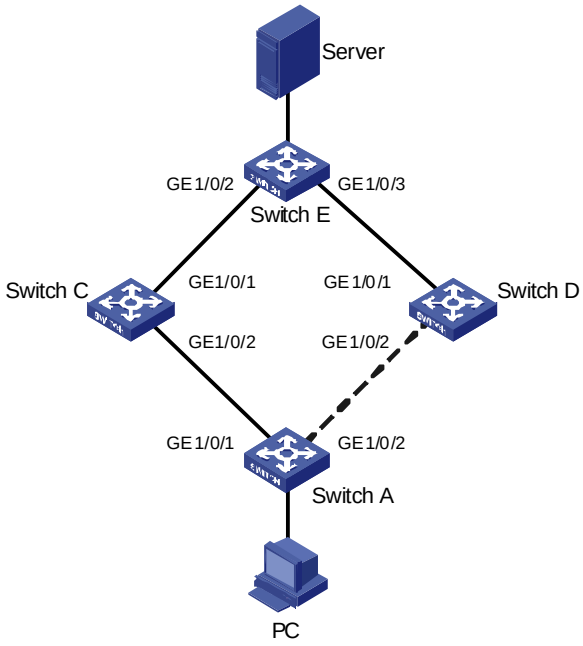
Smart Link Configuration Example

Implementing Link Redundancy Backup

Network requirements

As shown in Figure 1-3, Switch A is a WX3000 series device. Switch C, Switch D and Switch E support Smart Link. Configure Smart Link feature to provide remote PCs with reliable access to the server.

Figure 1-3 Network diagram for Smart Link configuration



Configuration procedure

1) Configure a Smart Link group on Switch A and configure member ports for it. Enable the function of sending flush messages in Control VLAN 1.

Enter system view.

```
<switchA> system-view
```

Enter Ethernet port view. Disable STP on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] stp disable
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] stp disable
```

Return to system view.

```
[SwitchA-GigabitEthernet1/0/2] quit
```

Create Smart Link group 1 and enter the corresponding Smart Link group view.

```
[SwitchA] smart-link group 1
```

Configure GigabitEthernet 1/0/1 as the master port and GigabitEthernet 1/0/2 as the slave port for Smart Link group 1.

```
[SwitchA-smlk-group1] port GigabitEthernet 1/0/1 master
[SwitchA-smlk-group1] port GigabitEthernet 1/0/2 slave
```

Configure to send flush messages within VLAN 1.

```
[SwitchA-smlk-group1] flush enable control-vlan 1
```

2) Enable the function of processing flush messages received from VLAN 1 on Switch C.

Enter system view.

```
<SwitchC> system-view
```

Enable the function of processing flush messages received from VLAN 1 on GigabitEthernet 1/0/2.

```
<SwitchC> smart-link flush enable control-vlan 1 port GigabitEthernet 1/0/2
```

3) Enable the function of processing flush messages received from VLAN 1 on Switch D.

Enter system view.

```
<SwitchD> system-view
```

Enable the function of processing flush messages received from VLAN 1 on GigabitEthernet 1/0/2.

```
[SwitchD] smart-link flush enable control-vlan 1 port GigabitEthernet 1/0/2
```

4) Enable the function of processing flush messages received from VLAN 1 on Switch E.

Enter system view.

```
<SwitchE> system-view
```

Enable the function of processing flush messages received from VLAN 1 on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[SwitchE] smart-link flush enable control-vlan 1 port GigabitEthernet 1/0/2 to GigabitEthernet 1/0/3
```

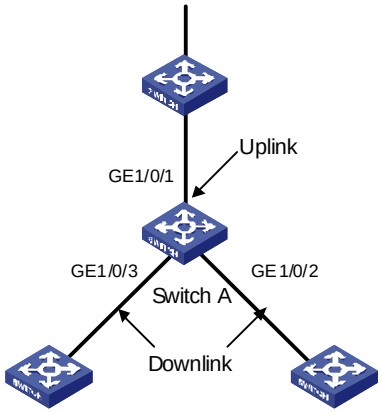
2 Monitor Link Configuration

Introduction to Monitor Link

Monitor Link is a collaboration scheme introduced to complement for Smart Link. It is used to monitor uplink and to perfect the backup function of Smart Link.

A monitor Link consists of an uplink port and one or multiple downlink ports. When the link for the uplink port of a Monitor Link group fails, all the downlink ports in the Monitor Link group are forced down. When the link for the uplink port recovers, all the downlink ports in the group are re-enabled.

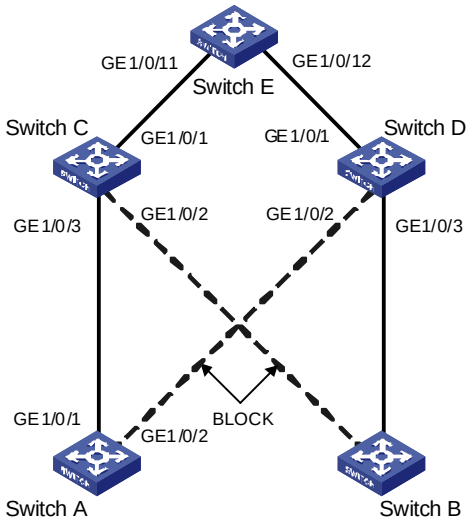
Figure 2-1 Network diagram for a Monitor Link group implementation



As shown in Figure 2-1, the Monitor Link group configured on the device Switch A consists of an uplink port (GigabitEthernet 1/0/1) and two downlink ports (GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3). A member port can be an Ethernet port, static LACP aggregation group, manual link aggregation group, or Smart Link group. A Smart Link group can serve as the uplink port only.

How Monitor Link Works

Figure 2-2 Network diagram for a Monitor Link group implementation



As shown in Figure 2-2, the devices Switch C and Switch D are connected to the uplink device Switch E. Switch C is configured with a Monitor Link group, where GigabitEthernet 1/0/1 is the uplink port, while GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are the downlink ports. Switch A is configured with a Smart Link group, where GigabitEthernet 1/0/1 is the master port and GigabitEthernet 1/0/2 is the slave port.

- If Switch C is not configured with Monitor Link group, when the link for the uplink port GigabitEthernet 1/0/1 on Switch C fails, the links in the Smart Link group are not switched because the link for the master port GigabitEthernet 1/0/1 of Switch A configured with Smart Link group operates normally. Actually, however, the traffic on Switch A cannot be up-linked to Switch E through the link of GigabitEthernet 1/0/1.
- If Switch C is configured with Monitor Link group and Monitor Link group detects that the link for the uplink port GigabitEthernet 1/0/1 fails, all the downlink ports in the group are shut down; therefore, GigabitEthernet 1/0/3 on Switch C is blocked. Now, Smart Link group configured on Switch A detects that a link fault occurs on the master port GigabitEthernet 1/0/1. Then, Smart Link immediately activates the slave port GigabitEthernet 1/0/2 so that traffic is switched to the backup link.

Note

- Currently, member ports of a Monitor Link group cannot be dynamic link aggregation groups.
- If the uplink or downlink port in the Monitor Link group is a link aggregation group, you cannot directly delete this aggregation group or change this aggregation group into a dynamic aggregation group. To delete this aggregation group, you must first unbind this aggregation group from the Monitor Link.

Configuring Monitor Link

Note

Before configuring a Monitor Link group, you must create a Monitor Link group and configure member ports for it. A Monitor Link group consists of an uplink port and one or multiple downlink ports. The uplink port can be a manually-configured or static LACP link aggregation group, an Ethernet port, or a Smart Link group. The downlink ports can be manually-configured link aggregation groups or static LACP link aggregation groups, or Ethernet ports.

Configuration Task List

Complete the following tasks to configure Monitor Link:

Task	Remarks
Creating a Monitor Link Group	Required
Configuring the Uplink Port	Required
Configuring a Downlink Port	Required

Creating a Monitor Link Group

Follow these steps to create a Monitor Link group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a Monitor Link group	**monitor-link group** *group-id*	Required

Configuring the Uplink Port

Follow these steps to configure the uplink port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter the specified Monitor Link group view	**monitor-link group** *group-id*	—

To do…			Use the command…	Remarks
Configure the uplink port for the Monitor Link group	Configure the specified link aggregation group as the uplink port of the Monitor Link group		**link-aggregation group** *group-id* **uplink**	Required Use any of the three approaches
	Configure the specified Smart Link group as the uplink port of the Monitor Link group		**smart-link group** *group-id* **uplink**	
	Configure the specified Ethernet port as the uplink port of the Monitor Link group	Monitor Link group view	**port** *interface-type interface-number* **uplink**	
		Ethernet port view	**quit**	
			interface *interface-type interface-number*	
			port monitor-link group *group-id* **uplink**	

Configuring a Downlink Port

Follow these steps to configure a downlink port:

To do…			Use the command…	Remarks
Enter system view			**system-view**	—
Enter the specified Monitor Link group view			**monitor-link group** *group-id*	Required
Configure a downlink port for the Monitor Link group	Configure the specified link aggregation group as a downlink port of the Monitor Link group		**link-aggregation group** *group-id* **downlink**	Required Use either approach
	Configure the specified Ethernet port as a downlink port of the Monitor Link group	Monitor Link group view	**port** *interface-type interface-number* **downlink**	
		Ethernet port view	**quit**	
			interface *interface-type interface-number*	
			port monitor-link group *group-id* **downlink**	

Caution

- A Smart Link/Monitor Link group with members cannot be deleted. A Smart Link group as a Monitor Link group member cannot be deleted.
- The Smart Link/Monitor Link function and the remote port mirroring function are incompatible with each other.
- If a single port is specified as a Smart Link/Monitor Link group member, do not use the **lacp enable** command on the port or add the port to another dynamic link aggregation group because doing so will cause the port to become an aggregation group member.
- Using the copy command on a port does not copy the Smart Link/Monitor Link group member information configured on the port to any other port.

Displaying and Maintaining Monitor Link

To do…	Use the command…	Remarks
Display the information about one or all Monitor Link groups	display monitor-link group { *group-id* | all }	Available in any view

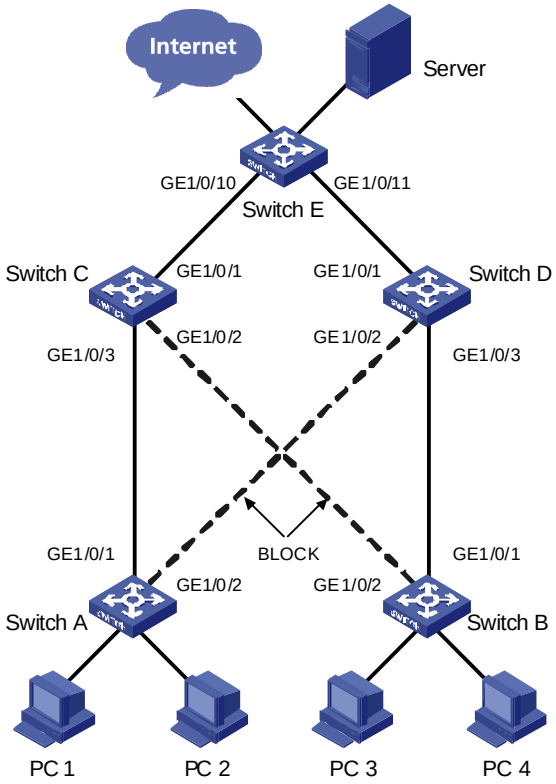
Monitor Link Configuration Example

Implementing Collaboration Between Smart Link and Monitor Link

Network requirements

As shown in Figure 2-3, the PCs access the server and Internet through the device. Configure Smart Link and Monitor Link to prevent the PCs from failing to access the server and Internet due to uplink link or port failure.

Figure 2-3 Network diagram for Monitor Link configuration



Configuration procedure

1) Enable Smart Link on Switch A and Switch B to implement link redundancy backup. Perform the following configuration on Switch A. The configuration on Switch B is the same as on Switch A.

Enter system view.

```
<switchA> system-view
```

Enter Ethernet port view. Disable STP on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] stp disable
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] stp disable
```

Return to system view.

```
[SwitchA-GigabitEthernet1/0/2] quit
```

Create Smart Link group 1 and enter Smart Link group view.

```
[SwitchA] smart-link group 1
```

Configure GigabitEthernet 1/0/1 as the master port of the Smart Link group and GigabitEthernet 1/0/2 as the slave port.

```
[SwitchA-smlk-group1] port GigabitEthernet 1/0/1 master
[SwitchA-smlk-group1] port GigabitEthernet 1/0/2 slave
```

Configure to send flush messages in VLAN 1.

```
[SwitchA-smlk-group1] flush enable control-vlan 1
```

2) Enable Monitor Link on Switch C and Switch D and enable the function of processing flush messages received from VLAN 1. Perform the following configuration on Switch C. The operation procedure on Switch D is the same as that performed on Switch C.

Enter system view.

```
<SwitchC> system-view
```

Create Monitor Link group 1 and enter Monitor Link group view

```
[SwitchC] monitor-link group 1
```

Configure GigabitEthernet 1/0/1 as the uplink port of the Monitor Link group and GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as the downlink ports.

```
[SwitchC-mtlk-group1] port GigabitEthernet 1/0/1 uplink
[SwitchC-mtlk-group1] port GigabitEthernet 1/0/2 downlink
[SwitchC-mtlk-group1] port GigabitEthernet 1/0/3 downlink
```

Return to system view. Enable the function of processing flush messages received from VLAN 1 on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[SwitchC-mtlk-group1] quit
[SwitchC] smart-link flush enable control-vlan 1 port GigabitEthernet 1/0/2 to GigabitEthernet 1/0/3
```

3) Enable the function of processing flush messages received from VLAN 1 on GigabitEthernet 1/0/10 and GigabitEthernet 1/0/11 of Switch E.

Enter system view.

```
<SwitchE> system-view
```

Enable the function of processing flush messages received from VLAN 1 on GigabitEthernet 1/0/10 and GigabitEthernet 1/0/11.

```
[SwitchE] smart-link flush enable control-vlan 1 port GigabitEthernet 1/0/10 to GigabitEthernet 1/0/11
```

Table of Contents

1 PoE Configuration 1-1

PoE Overview 1-1

Introduction to PoE 1-1

PoE Features Supported by the Device 1-2

PoE Configuration 1-2

PoE Configuration Task List 1-2

Enabling the PoE Feature on a Port 1-3

Setting the Maximum Output Power on a Port 1-3

Setting PoE Management Mode and PoE Priority of a Port 1-4

Setting the PoE Mode on a Port 1-4

Configuring the PD Compatibility Detection Function 1-5

Upgrading the PSE Processing Software Online 1-5

Displaying and Maintaining PoE Configuration 1-6

PoE Configuration Example 1-6

PoE Configuration Example 1-6

2 PoE Profile Configuration 2-1

Introduction to PoE Profile 2-1

PoE Profile Configuration 2-1

Configuring PoE Profile 2-1

Displaying and Maintaining PoE Profile Configuration 2-2

PoE Profile Configuration Example 2-3

PoE Profile Application Example 2-3

1 PoE Configuration

When configuring PoE, go to these sections for information you are interested in:

- PoE Overview
- PoE Configuration
- PoE Configuration Example

Note

The terms switching engine and Ethernet switch used throughout this documentation refer to a switching device in a generic sense or the switching engine of a unified switch in the WX3000 series.

PoE Overview

Introduction to PoE

Power over Ethernet (PoE)-enabled devices use twisted pairs through electrical ports to supply power to the remote powered devices (PD) in the network and implement power supply and data transmission simultaneously.

Advantages of PoE

- Reliability: The centralized power supply provides backup convenience, unified management, and safety.
- Easy connection: Network terminals only require an Ethernet cable, but no external power supply.
- Standard: PoE conforms to the 802.3af standard and uses a globally uniform power interfaces;
- Bright application prospect: PoE can be applied to IP phones, wireless access points (APs), chargers for portable devices, card readers, network cameras, and data collection system.

PoE components

PoE consists of three components: power sourcing equipment (PSE), PD, and power interface (PI).

- PSE: PSE is comprised of the power and the PSE functional module. It can implement PD detection, PD power information collection, PoE, power supply monitoring, and power-off for devices.
- PD: PDs receive power from the PSE. PDs include standard PDs and nonstandard PDs. Standard PDs conform to the 802.3af standard, including IP phones, Wireless APs, network cameras and so on.
- PI: PIs are RJ45 interfaces which connect PSE/PDs to network cables.

PoE Features Supported by the Device

Table 1-1 Power supply parameters of PoE device

Device	Input power supply	Number of electrical ports supplying power	Maximum PoE distance	Maximum power provided by each electrical port	Total Maximum PoE output power
WX3024	DC input	24	100 m (328.08 ft.)	25 W	600 W
	AC input				370 W
WX3010	DC input	8	100 m (328.08 ft.)	25 W	125 W
WX3008	DC input	4	100 m (328.08 ft.)	25 W	125 W

A PoE-enabled device has the following features:

- As the PSE, it supports the IEEE802.3af standard. It can also supply power to some PDs that do not support the 802.3af standard.
- It can deliver data and current simultaneously through data wires (1,2,3,6) of category-3/5 twisted pairs.
- The PSE processing software on the device can be upgraded online.
- The device provides statistics about power supplying on each port and the whole equipment, which you can query through the **display** command.
- The device provides two modes (**auto** and **manual**) to manage the power feeding to ports in the case of PSE power overload.
- The device provides over-temperature protection mechanism. When the internal temperature of the device exceeds the PoE protection temperature, the device disables the PoE feature on all ports for self-protection.
- The device supports the PoE profile feature, that is, different PoE policies can be set for different user groups. These PoE policies are each saved in the corresponding PoE profile and applied to ports of the user groups.

Note

- When you use the PoE-enabled device to supply power, the PDs need no external power supply.
- If a remote PD has an external power supply, the PoE-enabled device and the external power supply will backup each other for the PD.
- Only the Ethernet electrical ports of the PoE-enabled device support the PoE feature.

PoE Configuration

PoE Configuration Task List

Complete the following tasks to configure PoE:

Task	Remarks
Enabling the PoE Feature on a Port	Required
Setting the Maximum Output Power on a Port	Optional
Setting PoE Management Mode and PoE Priority of a Port	Optional
Setting the PoE Mode on a Port	Optional
Configuring the PD Compatibility Detection Function	Optional
Upgrading the PSE Processing Software Online	Optional
Displaying and Maintaining PoE Configuration	Optional

Enabling the PoE Feature on a Port

Follow these steps to enable the PoE feature on a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the PoE feature on a port	**poe enable**	Required

Caution

- By default, the PoE function on a port is enabled by the default configuration file when the device is delivered.
- If you delete the default configuration file without specifying another one, the PoE function on a port will be disabled after you restart the device.

Setting the Maximum Output Power on a Port

The maximum power that can be supplied by each Ethernet electrical port of a PoE-enabled device to its PD is 25,000 mW. In practice, you can set the maximum power on a port depending on the actual power of the PD, in the range of 1,000 to 25,000 mW and in the granularity of 1 mW.

Follow these steps to set the maximum output power on a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the maximum output power on the port	**poe max-power** *max-power*	Required 25,000 mW by default.

Setting PoE Management Mode and PoE Priority of a Port

When the device is close to its full load in supplying power, you can adjust the power supply of the device through the cooperation of the PoE management mode and the port PoE priority settings. The device supports two PoE management modes, auto and manual. The auto mode is adopted by default.

- **auto**: When the device is close to its full load in supplying power, it will first supply power to the PDs that are connected to the ports with critical priority, and then supply power to the PDs that are connected to the ports with high priority. For example: Port A has the priority of critical. When the device PoE is close to its full load and a new PD is now added to port A, the device will power down the PD connected to the port with the lowest priority and turn to supply power to this new PD. If more than one port has the same lowest priority, the device will power down the PD connected to the port with larger port number.
- **manual**: When the device is close to its full load in supplying power, it will not make change to its original power supply status based on its priority when a new PD is added. For example: Port A has the priority critical. When the device PoE is close to its full load and a new PD is now added to port A, the device just gives a prompt that a new PD is added and will not supply power to this new PD.

After the PoE feature is enabled on the port, perform the following configuration to set the PoE management mode and PoE priority of a port.

Follow these steps to set the PoE management mode and PoE priority of a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the PoE management mode for the device	**poe power-management** { **auto** | **manual** }	Required **auto** by default.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Se the PoE priority of a port	**poe priority** { **critical** | **high** | **low** }	Required **low** by default.

Setting the PoE Mode on a Port

PoE mode of a port falls into two types, signal mode and spare mode.

- Signal mode: DC power is carried over the data pairs (1,2,3,6) of category-3/5 twisted pairs.
- Spare mode: DC power is carried over the spare pairs (4,5,7,8) of category-3/5 twisted pairs.

Currently, the device does not support the spare mode.

After the PoE feature is enabled on the port, perform the following configuration to set the PoE mode on a port.

Follow these steps to set the PoE mode on a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

To do…	Use the command…	Remarks
Set the PoE mode on the port to signal	**poe mode signal**	Optional **signal** by default.

Configuring the PD Compatibility Detection Function

After the PD compatibility detection function is enabled, the device can detect the PDs that do not conform to the 802.3af standard and supply power to them.

After the PoE feature is enabled, perform the following configuration to enable the PD compatibility detection function.

Follow these steps to configure the PD compatibility detection function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the PD compatibility detection function	**poe legacy enable**	Required Disabled by default.

Upgrading the PSE Processing Software Online

The online upgrading of PSE processing software can update the processing software or repair the software if it is damaged. Before performing the following configuration, download the PSE processing software to the flash of the device .

Follow these steps to upgrade PSE processing software online:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Upgrade the PSE processing software online	**poe update** { **refresh** | **full** } *filename*	Required The specified PSE processing software is a file with the extension .s19.

Note

- In the case that the PSE processing software is damaged (that is, no **PoE** command can be executed successfully), use the **full** update mode to upgrade and thus restore the software.
- The **refresh** update mode is to upgrade the original processing software in the PSE through refreshing the software, while the **full** update mode is to delete the original processing software in PSE completely and then reload the software.
- Generally, the **refresh** update mode is used to upgrade the PSE processing software.
- When the online upgrading procedure is interrupted for some unexpected reason (for example, the device restarts due to some errors), if the upgrade in **full** mode fails after restart, you must upgrade in **full** mode after power-off and restart of the device, and then restart the device manually. In this way, the former PoE configuration is restored.

Displaying and Maintaining PoE Configuration

To do…	Use the command…	Remarks
Display the PoE status of a specific port or all ports of the device	**display poe interface** [*interface-type interface-number*]	Available in any view
Display the PoE power information of a specific port or all ports of the device	**display poe interface power** [*interface-type interface-number*]	
Display the PSE parameters	**display poe powersupply**	

PoE Configuration Example

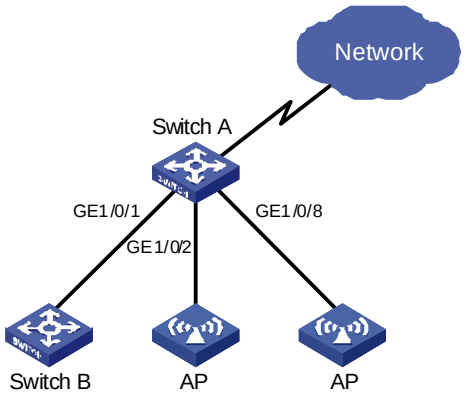
PoE Configuration Example

Networking requirements

As shown in Figure 1-1, Switch A supports PoE, Switch B can be PoE powered.

- The GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 ports of Switch A are connected to Switch B and an AP respectively; the GigabitEthernet 1/0/8 port is intended to be connected with an important AP.
- The PSE processing software of Switch A is first upgraded online. The remotely accessed PDs are powered by Switch A.
- The power consumption of the accessed AP is 2,500 mW, and the maximum power consumption of Switch B is 12,000 mW.
- It is required to guarantee the power feeding to the PDs connected to the GigabitEthernet 1/0/8 port even when Switch A is under full load.

Figure 1-1 Network diagram for PoE



Configuration procedure

Upgrade the PSE processing software online.

```
<SwitchA> system-view
[SwitchA] poe update refresh 0290_021.s19
```

Enable the PoE feature on GigabitEthernet 1/0/1, and set the PoE maximum output power of GigabitEthernet 1/0/1 to 12,000 mW.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] poe enable
[SwitchA-GigabitEthernet1/0/1] poe max-power 12000
[SwitchA-GigabitEthernet1/0/1] quit
```

Enable the PoE feature on GigabitEthernet 1/0/2, and set the PoE maximum output power of GigabitEthernet 1/0/2 to 2500 mW.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] poe enable
[SwitchA-GigabitEthernet1/0/2] poe max-power 2500
[SwitchA-GigabitEthernet1/0/2] quit
```

Enable the PoE feature on GigabitEthernet 1/0/8, and set the PoE priority of GigabitEthernet 1/0/8 to critical.

```
[SwitchA] interface GigabitEthernet 1/0/8
[SwitchA-GigabitEthernet1/0/8] poe enable
[SwitchA-GigabitEthernet1/0/8] poe priority critical
[SwitchA-GigabitEthernet1/0/8] quit
```

Set the PoE management mode on the device to auto (it is the default mode, so this step can be omitted).

```
[SwitchA] poe power-management auto
```

Enable the PD compatibility detect of the device to allow the device to supply power to part of the devices noncompliant with the 802.3af standard.

```
[SwitchA] poe legacy enable
```

2 PoE Profile Configuration

Introduction to PoE Profile

On a large-sized network or a network with mobile users, to help network administrators to monitor the PoE features of the device, the device provides the PoE profile features. A PoE profile is a set of PoE configurations, including multiple PoE features.

Features of PoE profile:

- Various PoE profiles can be created. PoE policy configurations applicable to different user groups are stored in the corresponding PoE profiles. These PoE profiles can be applied to the ports used by the corresponding user groups.
- When users connect a PD to a PoE-profile-enabled port, the PoE configurations in the PoE profile will be enabled on the port.

PoE Profile Configuration

Configuring PoE Profile

Follow these steps to configure PoE profile:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Create a PoE profile and enter PoE profile view		**poe-profile** *profilename*	Required If the PoE file is created, you will enter PoE profile view directly through the command.
Configure the relevant features in PoE profile	Enable the PoE feature on a port	**poe enable**	Required Disabled by default.
	Configure PoE mode for Ethernet ports	**poe mode** { **signal** | **spare** }	Optional **signal** by default.
	Configure the PoE priority for Ethernet ports	**poe priority** { **critical** | **high** | **low** }	Optional **low** by default.
	Configure the maximum power for Ethernet ports	**poe max-power** max-power	Optional 15,400 mW by default.
Quit system view		**quit**	—

To do…			Use the command…	Remarks
Apply the existing PoE profile to the specified Ethernet port	In system view		**apply poe-profile** *profile-name* **interface** *interface-type interface-number* [**to** *interface-type interface-number*]	Use either approach.
	In Ethernet port view	Enter Ethernet port view	**interface** *interface-type interface-number*	
		Apply the existing PoE profile to the port	**apply poe-profile** *profile-name*	

Note the following during the configuration:

1) When the **apply poe-profile** command is used to apply a PoE profile to a port, some PoE features in the PoE profile can be applied successfully while some cannot. PoE profiles are applied to the devices according to the following rules:

- When the **apply poe-profile** command is used to apply a PoE profile to a port, the PoE profile is applied successfully only if one PoE feature in the PoE profile is applied properly. When the **display current-configuration** command is used for query, it is displayed that the PoE profile is applied properly to the port.
- If one or more features in the PoE profile are not applied properly on a port, the device will prompt explicitly which PoE features in the PoE profile are not applied properly on which ports.
- The **display current-configuration** command can be used to query which PoE profile is applied to a port. However, the command cannot be used to query which PoE features in a PoE profiles are applied successfully.

2) PoE profile configuration is a global configuration, and applies synchronously in the intelligent resilient framework (IRF) system.

3) Combination of Unit creates a new Fabric. In the newly created Fabric, the PoE profile configuration of the Unit with the smallest Unit ID number will become the PoE profile configuration for the Fabric currently in use.

4) Split of Fabric results in many new Fabrics. In each newly created Fabric, the PoE profile configuration of each Unit remains the same as it was before the split.

Displaying and Maintaining PoE Profile Configuration

To do…	Use the command…	Remarks
Display the detailed information about the PoE profiles created on the device	**display poe-profile** { **all-profile** | **interface** *interface-type interface-number* | **name** *profile-name* }	Available in any view

PoE Profile Configuration Example

PoE Profile Application Example

Network requirements

As shown in Figure 2-1, Switch A supports PoE.

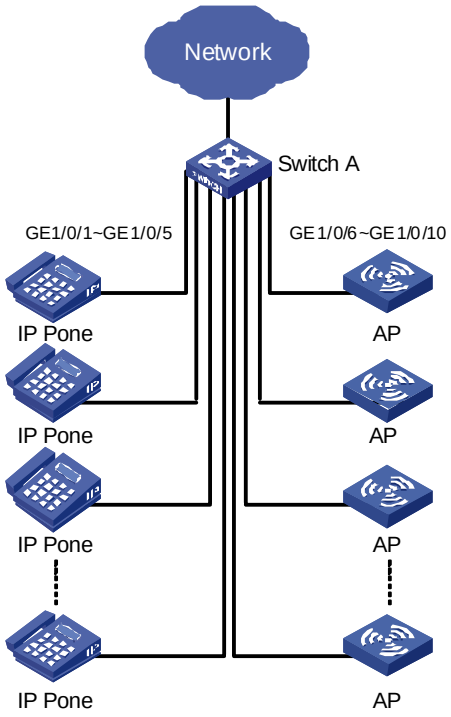
GigabitEthernet 1/0/1 through GigabitEthernet 1/0/10 of Switch A are used by users of group A, who have the following requirements:

- The PoE function can be enabled on all ports in use.
- Signal mode is used to supply power.
- The PoE priority for GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 is Critical, whereas the PoE priority for GigabitEthernet 1/0/6 through GigabitEthernet 1/0/10 is High.
- The maximum power for GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 ports is 3,000 mW, whereas the maximum power for GigabitEthernet 1/0/6 through GigabitEthernet 1/0/10 is 15,400 mW.

Based on the above requirements, two PoE profiles are made for users of group A.

- Apply PoE profile 1 for GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5;
- Apply PoE profile 2 for GigabitEthernet 1/0/6 through GigabitEthernet 1/0/10.

Figure 2-1 PoE profile application



Configuration procedure

Create Profile1, and enter PoE profile view.

```
<SwitchA> system-view
[SwitchA] poe-profile Profile1
```

In Profile1, add the PoE policy configuration applicable to GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 ports for users of group A.

```
[SwitchA-poe-profile-Profile1] poe enable
[SwitchA-poe-profile-Profile1] poe mode signal
[SwitchA-poe-profile-Profile1] poe priority critical
[SwitchA-poe-profile-Profile1] poe max-power 3000
[SwitchA-poe-profile-Profile1] quit
```

Display detailed configuration information for Profile1.

```
[SwitchA] display poe-profile name Profile1
Poe-profile: Profile1, 3 action
poe enable
poe max-power 3000
poe priority critical
```

Create Profile2, and enter PoE profile view.

```
[SwitchA] poe-profile Profile2
```

In Profile2, add the PoE policy configuration applicable to GigabitEthernet 1/0/6 through GigabitEthernet 1/0/10 ports for users of group A.

```
[SwitchA-poe-profile-Profile2] poe enable
[SwitchA-poe-profile-Profile2] poe mode signal
[SwitchA-poe-profile-Profile2] poe priority high
[SwitchA-poe-profile-Profile2] poe max-power 15400
[SwitchA-poe-profile-Profile2] quit
```

Display detailed configuration information for Profile2.

```
[SwitchA] display poe-profile name Profile2
Poe-profile: Profile2, 2 action
poe enable
poe priority high
```

Apply the configured Profile1 to GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 ports.

```
[SwitchA] apply poe-profile Profile1 interface GigabitEthernet1/0/1 to GigabitEthernet1/0/5
```

Apply the configured Profile2 to GigabitEthernet 1/0/6 through GigabitEthernet 1/0/10 ports.

```
[SwitchA] apply poe-profile Profile2 interface GigabitEthernet1/0/6 to
GigabitEthernet1/0/10
```

Table of Contents

1 IP Routing Protocol Overview 1-1
Introduction to IP Route and Routing Table 1-1
IP Route 1-1
Routing Table 1-1
Routing Protocol Overview 1-3
Static Routing and Dynamic Routing 1-3
Classification of Dynamic Routing Protocols 1-3
Routing Protocols and Routing Priority 1-3
Load Sharing and Route Backup 1-4
Routing Information Sharing 1-4
Displaying and Maintaining a Routing Table 1-5

2 Static Route Configuration 2-1
Introduction to Static Route 2-1
Static Route 2-1
Default Route 2-2
Static Route Configuration 2-2
Configuration Prerequisites 2-2
Configuring a Static Route 2-2
Displaying and Maintaining Static Routes 2-3
Static Route Configuration Example 2-3
Troubleshooting a Static Route 2-4

3 RIP Configuration 3-1
RIP Overview 3-1
Basic Concepts 3-1
RIP Startup and Operation 3-2
RIP Configuration Task List 3-3
Basic RIP Configuration 3-3
Configuration Prerequisites 3-3
Configuring Basic RIP Functions 3-3
RIP Route Control 3-4
Configuration Prerequisites 3-5
Configuring RIP Route Control 3-5
RIP Network Adjustment and Optimization 3-7
Configuration Prerequisites 3-8
Configuration Tasks 3-8
Displaying and Maintaining RIP Configuration 3-10
RIP Configuration Example 3-10
Troubleshooting RIP Configuration 3-11
Failed to Receive RIP Updates 3-11

4 IP Route Policy Configuration 4-1
IP Route Policy Overview 4-1
Introduction to IP Route Policy 4-1

Filters ····· 4-1
IP Route Policy Configuration Task List ····· 4-2
Route Policy Configuration ····· 4-2
Configuration Prerequisites ····· 4-2
Defining a Route Policy ····· 4-3
Defining if-match Clauses and apply Clauses ····· 4-3
Displaying and Maintaining IP Route Policy ····· 4-4
IP Route Policy Configuration Example ····· 4-4
Controlling RIP Packet Cost to Implement Dynamic Route Backup ····· 4-4
Troubleshooting IP Route Policy ····· 4-8

1 IP Routing Protocol Overview

Go to these sections for information you are interested in:

- Introduction to IP Route and Routing Table
- Routing Protocol Overview
- Displaying and Maintaining a Routing Table

Note

The term **router** in this chapter refers to a router in a generic sense or a WX3000 series device running a routing protocol.

Introduction to IP Route and Routing Table

IP Route

Routers are used for route selection on the Internet. As a router receives a packet, it selects an appropriate route (through a network) according to the destination address of the packet and forwards the packet to the next router. The last router on the route is responsible for delivering the packet to the destination host.

Routing Table

Function

The key for a router to forward packets is the routing table. Each router maintains a routing table. Each entry in this table contains an IP address that represents a host/subnet and specifies which physical port on the router should be used to forward the packets destined for the host/subnet. And the router forwards those packets through this port to the next router or directly to the destination host if the host is on a network directly connected to the router.

Routes in a routing table can be divided into three categories by origin:

- Direct routes: Routes discovered by data link protocols, also known as interface routes.
- Static routes: Routes that are manually configured.
- Dynamic routes: Routes that are discovered dynamically by routing protocols.

Routing entry

Each routing entry in a routing table contains:

- Destination: It identifies the address of the destination host or network of an IP packet.
- Mask: Along with the destination address, it identifies the address of the network segment where the destination host or router resides. By performing a logical AND operation between destination address and network mask, you can get the address of the network segment where the destination

host or router resides. For example, if the destination address is 129.102.8.10 and the mask is 255.255.0.0, the address of the network segment where the destination host or router resides is 129.102.0.0. A mask consists of some consecutive 1s, represented either in dotted decimal notation or by the number of the consecutive 1s in the mask.

- Interface: It indicates through which interface IP packets should be forwarded to the destination.
- Nexthop: It indicates the next router that IP packets will pass through to reach the destination.
- Preference: There may be multiple routes with different next hops to the same destination. These routes may be discovered by different routing protocols, or be manually configured static routes. The one with the highest preference (the smallest numerical value) will be selected as the current optimal route.

According to different destinations, routes fall into the following categories:

- Subnet route: The destination is a subnet.
- Host route: The destination is a host.

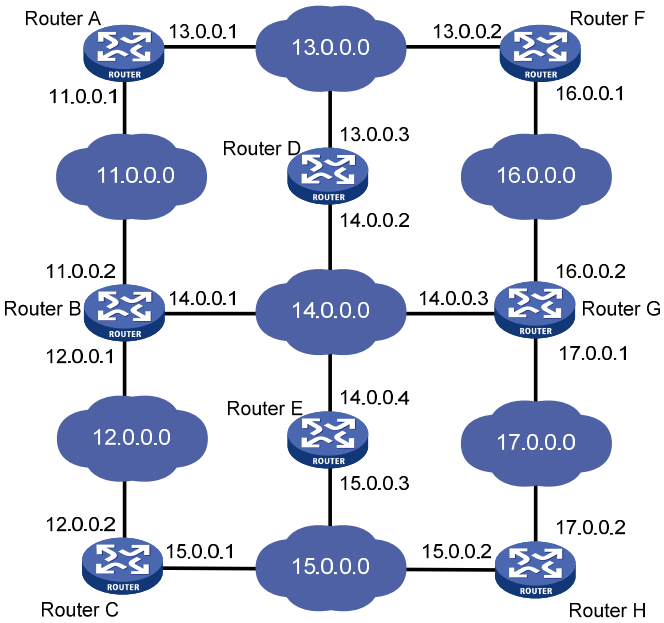
In addition, according to whether the network where the destination resides is directly connected to the router, routes fall into the following categories:

- Direct route: The router is directly connected to the network where the destination resides.
- Indirect route: The router is not directly connected to the network where the destination resides.

In order to avoid an oversized routing table, you can set a default route. All the packets for which the router fails to find a matching entry in the routing table will be forwarded through this default route.

Figure 1-1 shows a relatively complicated internet environment, the number in each network cloud indicate the network address. Router G is connected to three networks, and so it has three IP addresses and three physical ports. Its routing table is shown in Figure 1-1.

Figure 1-1 Routing table



Destination Network	Nexthop	Interface
11.0.0.0	14.0.0.1	3
12.0.0.0	14.0.0.1	3
13.0.0.0	16.0.0.1	2
14.0.0.0	14.0.0.3	3
15.0.0.0	17.0.0.2	1
16.0.0.0	16.0.0.2	2
17.0.0.0	17.0.0.1	1

Routing Protocol Overview

Static Routing and Dynamic Routing

Static routing is easy to configure and requires less system resources. It works well in small, stable networks with simple topologies. It cannot adapt itself to any network topology change automatically so that you must perform routing configuration again whenever the network topology changes.

Dynamic routing is based on dynamic routing protocols, which can detect network topology changes and recalculate the routes accordingly. Therefore, dynamic routing is suitable for large networks. It is complicated to configure, and it not only imposes higher requirements on the system than static routing, but also occupies a certain amount of network resources.

Classification of Dynamic Routing Protocols

Dynamic routing protocols can be classified based on the following standards:

Operational scope

- Interior Gateway Protocols (IGPs): Work within an autonomous system, typically including RIP, OSPF, and IS-IS.
- Exterior Gateway Protocols (EGPs): Work between autonomous systems. The most popular one is BGP.



Note

An autonomous system refers to a group of routers that share the same route policy and work under the same administration.

Routing algorithm

- Distance-vector protocols: RIP and BGP. BGP is also considered a path-vector protocol.
- Link-state protocols: OSPF and IS-IS.

The main differences between the above two types of routing algorithms lie in the way routes are discovered and calculated.

Type of the destination address

- Unicast routing protocols: RIP, OSPF, BGP, and IS-IS.
- Multicast routing protocols: PIM-SM and PIM-DM.

This chapter focuses on unicast routing protocols. For information on multicast routing protocols, refer to the part discussing *Multicast*.

Routing Protocols and Routing Priority

Different routing protocols may find different routes (including static routes) to the same destination. However, not all of those routes are optimal. In fact, at a particular moment, only one protocol can uniquely determine the current optimal routing to the destination. For the purpose of route selection,

each routing protocol (including static routes) is assigned a priority. The route found by the routing protocol with the highest priority is preferred.

The following table lists some routing protocols and the default priorities for routes found by them:

Table 1-1 Routing protocols and priorities of their default route

Routing approach	Priority
DIRECT	0
OSPF	10
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
UNKNOWN	255

Note

- The smaller the priority value, the higher the priority.
- The priority for a direct route is always 0, which you cannot change. Any other type of routes can have their priorities manually configured.
- Each static route can be configured with a different priority.

Load Sharing and Route Backup

Load sharing

A given routing protocol may find several routes with the same metric to the same destination, and if this protocol has the highest priority among all the active protocols, these routes will be considered valid and are used to forward packets, thus achieving load sharing.

Route backup

You can configure multiple routes to the same destination, expecting the one with the highest priority to be the primary route and all the rest backup routes.

Route backup can help improve network reliability. Automatic switching can happen between the primary route and a backup route.

Under normal circumstances, packets are forwarded through the primary route. When the primary route goes down, the route with the highest priority among the backup routes is selected to forward packets. When the primary route recovers, the route selection process is performed again and the primary route is selected again to forward packets.

Routing Information Sharing

As different routing protocols use different algorithms to calculate routes, they may discover different routes. In a large network with multiple routing protocols, it is required for routing protocols to share their

routing information. Each routing protocol shares routing information discovered by other routing protocols through a route redistribution mechanism.

Displaying and Maintaining a Routing Table

To do…	Use the command…	Remarks
Display brief information about a routing table	**display ip routing-table** [**|** { **begin | exclude | include** } *regular-expression*]	Available in any view
Display detailed information about a routing table	**display ip routing-table verbose**	
Display information about routes permitted by a basic ACL	**display ip routing-table acl** *acl-number* [**verbose**]	
Display information about routes permitted by a prefix list	**display ip routing-table ip-prefix** *ip-prefix-name* [**verbose**]	
Display routes to a specified destination	**display ip routing-table** *ip-address* [*mask* | *mask-length*] [**longer-match**] [**verbose**]	
Display routes to specified destinations	**display ip routing-table** *ip-address1* { *mask1* | *mask-length1* } *ip-address2* { *mask2* | *mask-length2* } [**verbose**]	
Display routes discovered by a routing protocol	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**]	
Display the tree-structured routing table information	**display ip routing-table radix**	
Display statistics about a routing table	**display ip routing-table statistics**	
Clear statistics about a routing table	**reset ip routing-table statistics protocol** { **all** | *protocol* }	Available in user view

2 Static Route Configuration

When configuring a static route, go to these sections for information you are interested in:

- Introduction to Static Route
- Static Route Configuration
- Displaying and Maintaining Static Routes
- Static Route Configuration Example
- Troubleshooting a Static Route



Note

The term **router** in this chapter refers to a router in a generic sense or a WX3000 series device running a routing protocol.

Introduction to Static Route

Static Route

Static routes are special routes. They are manually configured by the administrator. In a relatively simple network, you only need to configure static routes to make routers work normally. Proper configuration and usage of static routes can improve network performance and ensure sufficient bandwidth for important applications.

When the network topology changes, static routes may become unreachable because they cannot adapt themselves to the change automatically, thus resulting in network interruption. In this case, the network administrator needs to modify the configuration of static routes manually.

Static routes are divided into three types:

- Reachable route: normal route. If a static route to a destination is of this type, the IP packets destined for this destination will be forwarded to the next hop. It is the most common type of static routes.
- Unreachable route: route with the **reject** attribute. If a static route to a destination has the **reject** attribute, all the IP packets destined for this destination will be discarded, and the source hosts will be informed of the unreachability of the destination.
- Blackhole route: route with **blackhole** attribute. If a static route destined for a destination has the **blackhole** attribute, the outgoing interface of this route is the Null 0 interface regardless of the next hop address, and all the IP packets addressed to this destination will be dropped without notifying the source hosts.

The attributes **reject** and **blackhole** are usually used to limit the range of the destinations this router can reach, and help troubleshoot the network.

Default Route

To avoid too large a routing table, you can configure a default route.

When the destination address of a packet fails to match any entry in the routing table,

- If there is default route in the routing table, the default route will be selected to forward the packet.
- If there is no default route, the packet will be discarded and an ICMP Destination Unreachable or Network Unreachable packet will be returned to the source.

A default route can be manually configured or generated by some dynamic routing protocols, such as OSPF and RIP.

Static Route Configuration

Configuration Prerequisites

Before configuring a static route, perform the following tasks:

- Configuring the physical parameters of related interfaces
- Configuring IP addresses for related interfaces

Configuring a Static Route

Follow these steps to configure a static route:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure a static route	**ip route-static** *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-hop* } [**preference** *preference-value*] [**reject** | **blackhole**] [**detect-group** *group number*] [**description** *text*]	Required By default, the system can obtain the route to the subnet directly connected to the router.



Note

- Use the **ip route-static** command to configure a default route by setting the destination IP address and the mask to 0.0.0.0.
- Avoid configuring the next hop address of a static route to the address of an interface on the local device.
- Different preferences can be configured to implement flexible route management policies.
- For automatic detection information, refer to the part discussing *Auto Detect*.

Displaying and Maintaining Static Routes

To do...	Use the command...	Remarks
Display the current configuration information	**display current-configuration**	Available in any view
Display the brief information of a routing table	**display ip routing-table**	
Display the detailed information of a routing table	**display ip routing-table verbose**	
Display the information of static routes	**display ip routing-table protocol static** [**inactive** | **verbose**]	
Delete all static routes	**delete static-routes all**	Available in system view

Static Route Configuration Example

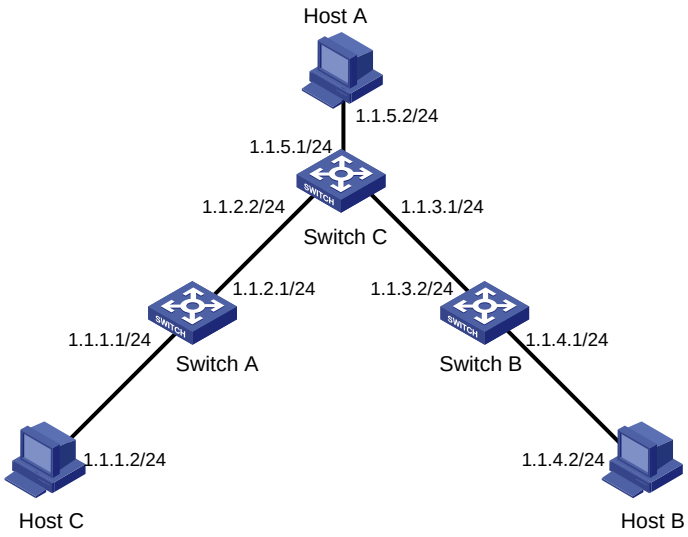
Network requirements

A small company requires that any two nodes in its office network communicate with each other, and that the network structure be simple and stable. The company hopes that the existing devices that do not support any dynamic routing protocol can be fully utilized.

In this case, static routes can implement communication between any two nodes.

According to the network requirements, the network topology is designed as shown in Figure 2-1.

Figure 2-1 Network diagram for static route configuration



Configuration procedure

Note

When only one interface of the device is interconnected with another network segment, you can implement network communication by configuring either a static route or default route.

1) Perform the following configurations on the device.

Approach 1: Configure static routes on Switch A.

```
<SwitchA> system-view
[SwitchA] ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

Approach 2: Configure a static route on Switch A.

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.2.2
```

Approach 1: Configure static routes on Switch B.

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

Approach 2: Configure a static route on Switch B.

```
<SwitchB> system-view
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 1.1.3.1
```

Configure static routes on Switch C.

```
<SwitchC> system-view
[SwitchC] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[SwitchC] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

2) Perform the following configurations on the host.

Set the default gateway address of Host A to 1.1.5.1. Detailed configuration procedure is omitted.

Set the default gateway address of Host B to 1.1.4.1. Detailed configuration procedure is omitted.

Set the default gateway address of Host C to 1.1.1.1. Detailed configuration procedure is omitted.

Now, all the hosts and devices in the figure can communicate with each other.

Troubleshooting a Static Route

Symptom: The device is not configured with a dynamic routing protocol. Both the physical status and the link layer protocol status of an interface are up, but IP packets cannot be forwarded on the interface.

Solution: Perform the following procedure.

1) Use the **display ip routing-table protocol static** command to view whether the corresponding static route is correctly configured.
2) Use the **display ip routing-table** command to view whether the static route is valid.

3 RIP Configuration

When configuring RIP, go to these sections for information you are interested in:

- RIP Overview
- RIP Configuration Task List
- RIP Configuration Example
- Troubleshooting RIP Configuration



Note

The term **router** in this chapter refers to a router in a generic sense or a WX3000 series device running a routing protocol.

RIP Overview

Routing information protocol (RIP) is a simple interior gateway protocol (IGP) suitable for small-sized networks. RIP is not recommended in complicated large networks.

Basic Concepts

RIP

RIP is a distance-vector (D-V) algorithm–based protocol. It uses port 520 to exchange routing information through UDP packets.

RIP uses hop count (also called routing cost) to measure the distance to a destination address. In RIP, the hop count from a router to its directly connected network is 0, and that to a network which can be reached through another router is 1, and so on. To restrict the time to converge, RIP prescribes that the cost is an integer ranging from 0 and 15. The hop count equal to or exceeding 16 is defined as infinite; that is, the destination network or host is unreachable. This limitation makes RIP not suitable for large networks.

To improve performance and avoid routing loop, RIP supports split horizon. Besides, RIP can import routes discovered by other routing protocols.

RIP routing database

Each RIP router has a routing table containing routing entries of all reachable destinations, and each routing entry contains:

- Destination address: IP address of a host or network.
- Next hop: IP address of an interface on the adjacent router that IP packets should pass through to reach the destination.

- Interface: Outbound interface on this router, through which IP packets should be forwarded to reach the destination.
- Metric: Cost from the local router to the destination.
- Route time: Time elapsed since the routing entry was last updated. The time is reset to 0 every time the routing entry is updated.

RIP timers

As defined in RFC 1058, RIP is controlled by three timers: Period update, Timeout, and Garbage-collection.

- Period update timer: The period update timer defines the interval between routing updates.
- Timeout timer: The timeout timer defines the route aging time. If no update for a route is received after the aging time elapses, the metric of the route is set to 16 in the routing table.
- Garbage-collection timer: The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the Garbage-Collect timer length, RIP advertises the route with the routing metric set to 16. If no update is announced for that route after the Garbage-Collect timer expires, the route will be deleted from the routing table.

Routing loops prevention

RIP is a distance-vector (D-V) based routing protocol. Since a RIP router advertises its own routing table to neighbors, routing loops may occur.

RIP uses the following mechanisms to prevent routing loops.

- Counting to infinity. The metric value of 16 is defined as unreachable. When a routing loop occurs, the metric value of the route will increment to 16.
- Split horizon. A router does not send the routing information learned from a neighbor back to the neighbor to prevent routing loops and save the bandwidth.

RIP Startup and Operation

The whole process of RIP startup and operation is as follows:

- Once RIP is enabled on a router, the router broadcasts or multicasts a request packet to its neighbors. Upon receiving the packet, each neighbor running RIP answers a response packet containing its routing table information.
- When this router receives a response packet, it updates its local routing table and sends a triggered update packet to the neighbors. Upon receiving the triggered update packet, the neighbor sends the packet to all its neighbors. After a series of update triggering processes, each router can get and keep the updated routing information.
- By default, RIP sends its routing table to its neighbors every 30 seconds. Upon receiving the packets, the neighbors maintain their own routing tables and select optimal routes, and then advertise update information to their respective neighbors so as to make the updated routes known globally. Furthermore, RIP uses the aging mechanism to handle the timeout routes to ensure real-time and valid routes.

RIP Configuration Task List

Complete the following tasks to configure RIP:

Task		Remarks
Configuring Basic RIP Functions	Enabling RIP on the interfaces attached to a specified network segment	Required
	Setting the RIP operating status on an interface	Optional
	Specifying the RIP version on an interface	Optional
Configuring RIP Route Control	Setting the additional routing metrics of an interface	Optional
	Configuring RIP route summarization	Optional
	Disabling the router from receiving host routes	Optional
	Configuring RIP to filter incoming/outgoing routes	Optional
	Setting RIP preference	Optional
	Configuring RIP to redistribute routes from another protocol	Optional
RIP Network Adjustment and Optimization	Configuring RIP timers	Optional
	Configuring split horizon	Optional
	Configuring RIP-1 packet zero field check	Optional
	Setting RIP-2 packet authentication mode	Optional
	Configuring RIP to unicast RIP packets	Optional

Basic RIP Configuration

Configuration Prerequisites

Before configuring basic RIP functions, perform the following tasks:

- Configuring the link layer protocol
- Configuring the network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer

Configuring Basic RIP Functions

Enabling RIP on the interfaces attached to a specified network segment

Follow these steps to enable RIP on the interfaces attached to a specified network segment:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable RIP and enter RIP view	**rip**	Required
Enable RIP on the specified interface	**network** *network-address*	Required Disabled by default

Note

- Related RIP commands configured in interface view can take effect only after RIP is enabled.
- RIP operates on the interfaces attached to a specified network segment. When RIP is disabled on an interface, it does not operate on the interface, that is, it neither receives/sends routes on the interface, nor forwards any interface route. Therefore, after RIP is enabled globally, you must also specify its operating network segments to enable it on the corresponding interfaces.

Setting the RIP operating status on an interface

Follow these steps to set the RIP operating status on an interface:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Enable the interface to receive RIP update packets	**rip input**	Optional Enabled by default
Enable the interface to send RIP update packets	**rip output**	
Enable the interface to receive and send RIP update packets	**rip work**	

Specifying the RIP version on an interface

Follow these steps to specify the RIP version on an interface:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Specify the version of the RIP running on the interface	**rip version** { **1** | **2** [**broadcast** | **multicast**] }	Optional By default, the version of the RIP running on an interface is RIP-1.

RIP Route Control

In actual implementation, it may be needed to control RIP routing information more accurately to accommodate complex network environments. By performing the configuration described in the following sections, you can:

- Control route selection by adjusting additional routing metrics on interfaces running RIP.
- Reduce the size of the routing table by setting route summarization and disabling the receiving of host routes.
- Filter incoming and outgoing routes.

- Set the preference of RIP to change the preference order of routing protocols. This order makes sense when more than one route to the same destination is discovered by multiple routing protocols.
- Redistribute external routes in an environment with multiple routing protocols.

Configuration Prerequisites

Before configuring RIP route control, perform the following tasks:

- Configuring network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer
- Configuring basic RIP functions

Configuring RIP Route Control

Setting the additional routing metrics of an interface

Additional metric is the metric added to the original metrics of RIP routes on an interface. It does not directly change the metric value of a RIP route in the routing table of a router, but will be added to incoming or outgoing RIP routes on the interface.

Follow these steps to set additional routing metric:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Set the additional routing metric to be added for incoming RIP routes on this interface	**rip metricin** *value*	Optional 0 by default
Set the additional routing metric to be added for outgoing RIP routes on this interface	**rip metricout** *value*	Optional 1 by default

Note

The **rip metricout** command takes effect only on the RIP routes learnt by the router and the RIP routes generated by the router itself, but the command is invalid for any route imported to RIP from other routing protocols.

Configuring RIP route summarization

Rip route summarization means that when the router advertises RIP updates, different subnet routes in the same natural network segment can be aggregated into one route with a natural mask for transmission to another network segment. This function is used to reduce the routing traffic on the network as well as the size of the routing table.

When it is necessary to advertise RIP route updates in a subnet, disable the route summarization for RIP-2.

Follow these steps to configure RIP route summarization:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Enable RIP-2 automatic route summarization	**summary**	Required Enabled by default

Disabling the router from receiving host routes

In some special cases, the router can receive a lot of host routes from the same segment, and these routes are of little help in route addressing but consume a lot of network resources. After a router is disabled from receiving host routes, it can refuse any incoming host route.

Follow these steps to disable the router from receiving host routes:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Disable the router from receiving host routes	**undo host-route**	Required By default, the router receives host routes.

Configuring RIP to filter incoming/outgoing routes

The route filtering function provided by a router enables you to configure inbound/outbound filter policy by specifying an ACL, address prefix list, or route policy to make RIP filter incoming/outgoing routes. Besides, you can configure RIP to receive only the RIP packets from a specific neighbor.

Follow these steps to configure RIP to filter incoming/outgoing routes:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Configure RIP to filter incoming routes	**filter-policy** { *acl-number* | **route-policy** *route-policy-name* } **import**	Required By default, RIP does not filter any incoming route.
	filter-policy gateway *ip-prefix-name* **import**	
Configure RIP to filter outgoing routes	**filter-policy** *acl-number* **export** [*protocol* [*process-id*]]	Required By default, RIP does not filter any outgoing route.
	filter-policy route-policy *route-policy-name* **export**	

Note

- The **filter-policy import** command filters the RIP routes received from neighbors, and the routes being filtered out will neither be added to the routing table nor be advertised to any neighbors.
- The **filter-policy export** command filters all the routes to be advertised, including the routes redistributed with the **import-route** command and routes learned from neighbors.
- You can also use the **filter-policy export** command to filter outgoing routes redistributed from a specified routing protocol.

Setting RIP preference

Follow these steps to set RIP preference:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Set the RIP preference	**preference** *value*	Required 100 by default

Configuring RIP to redistribute routes from another protocol

Follow these steps to configure RIP to import routes from another protocol:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Configure a default cost for an incoming route	**default cost** *value*	Optional 1 by default
Configure RIP to redistribute routes from another protocol	**import-route** *protocol* [*process-id*] [**cost** *value* | **route-policy** *route-policy-name*]*	Required By default, RIP does not redistribute any route from other protocols.

RIP Network Adjustment and Optimization

In some special network environments, some RIP features need to be configured and RIP network performance needs to be adjusted and optimized. By performing the configuration mentioned in this section, the following can be implemented:

- Changing the convergence speed of RIP network by adjusting RIP timers;
- Avoiding routing loops by configuring split horizon;
- Packet validation in network environments with high security requirements, and
- Configuring RIP to unicast RIP messages on interfaces with special requirements.

Configuration Prerequisites

Before adjusting RIP, perform the following tasks:

- Configuring the network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer
- Configuring basic RIP functions

Configuration Tasks

Configuring RIP timers

Follow these steps to configure RIP timers:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Set the RIP timers	**timers** { **update** *update-timer* | **timeout** *timeout-timer* } *	Required By default, the Update timer is 30 seconds and the Timeout timer 180 seconds.

Note

When configuring the values of RIP timers, you should take network performance into consideration and perform consistent configuration on all routers running RIP to avoid unnecessary network traffic and network route oscillation.

Configuring split horizon

Follow these steps to configure split horizon:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Enable split horizon	**rip split-horizon**	Required Enabled by default

Note

Split horizon cannot be disabled on a point-to-point link.

Configuring RIP-1 packet zero field check

Follow these steps to configure RIP-1 packet zero field check:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Enable the check of the **must be zero** field in RIP-1 packets	**checkzero**	Required Enabled by default

Note

Some fields in a RIP-1 packet must be 0, and they are known as **must be zero** field. For RIP-1, the **must be zero** field is checked for incoming packets, and those RIP-1 packets with this field being nonzero will not be processed.

Setting RIP-2 packet authentication mode

RIP-2 supports two authentication modes: simple authentication and message digest 5 (MD5) authentication.

Simple authentication cannot provide complete security, because the authentication keys sent along with packets that are not encrypted. Therefore, simple authentication cannot be applied where high security is required.

Follow these steps to set RIP-2 packet authentication mode:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Set RIP-2 packet authentication mode	**rip authentication-mode** { **simple** *password* | **md5** { **rfc2082** *key-string key-id* | **rfc2453** *key-string* } }	Required If you specify to use MD5 authentication, you must specify one of the following MD5 authentication types: • rfc2453 (this type supports the packet format defined in RFC 2453) • rfc2082 (this type supports the packet format defined in RFC 2082)

Configuring RIP to unicast RIP packets

Follow these steps to configure RIP to unicast RIP packets:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—

To do...	Use the command...	Remarks
Configure RIP to unicast RIP packets	**peer** *ip-address*	Required When RIP runs on the link that does not support broadcast or multicast, you must configure RIP to unicast RIP packets.

Displaying and Maintaining RIP Configuration

To do...	Use the command...	Remarks
Display the current RIP running status and configuration information	**display rip**	Available in any view
Display RIP interface information	**display rip interface**	
Display RIP routing information	**display rip routing**	
Reset the system configuration related to RIP	**reset**	Available in RIP view

RIP Configuration Example

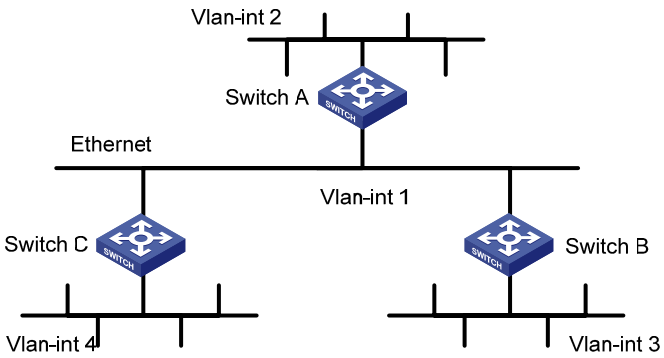
Network requirements

A small-sized company requires that any two nodes in its small office network communicate with each other, and that the network devices automatically adapt themselves to any topology change so as to reduce the work of manual maintenance.

In this case, RIP can implement communication between any two nodes.

According to the network requirements, the network topology is designed as shown in Figure 3-1.

Figure 3-1 Network diagram for RIP configuration



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int1	110.11.2.1/24	Switch B	Vlan-int1	110.11.2.2/24
	Vlan-int2	155.10.1.1/24		Vlan-int3	196.38.165.1/24
Switch C	Vlan-int1	110.11.2.3/24			
	Vlan-int4	117.102.0.1/16			

Configuration procedure

Note

Only the configuration related to RIP is listed below. Before the following configuration, make sure the Ethernet link layer works normally and the IP addresses of VLAN interfaces are configured correctly.

1) Configure Switch A:

Configure RIP.

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip] network 110.11.2.0
[SwitchA-rip] network 155.10.1.0
```

2) Configure Switch B:

Configure RIP.

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip] network 196.38.165.0
[SwitchB-rip] network 110.11.2.0
```

3) Configure Switch C:

Configure RIP.

```
<SwitchC> system-view
[SwitchC] rip
[SwitchC-rip] network 117.102.0.0
[SwitchC-rip] network 110.11.2.0
```

Troubleshooting RIP Configuration

Failed to Receive RIP Updates

Symptom

The device cannot receive any RIP update when the physical connection between the device and the peer routing device is normal.

Solution

Check that:

- RIP is enabled by using the **network** command on the corresponding interface.
- The interface is allowed to receive or send RIP packets.
- The interface receives RIP packets in the way the peer device sends them, for example, in the broadcast or multicast mode.

4 IP Route Policy Configuration

When configuring an IP route policy, go to these sections for information you are interested in:

- IP Route Policy Overview
- IP Route Policy Configuration Task List
- Displaying and Maintaining IP Route Policy
- IP Route Policy Configuration Example
- Troubleshooting IP Route Policy



Note

The term **router** in this chapter refers to a router in a generic sense or a WX3000 series device running a routing protocol.

IP Route Policy Overview

Introduction to IP Route Policy

Route policy is technology used to modify routing information to control the forwarding path of data packets. Route policy is implemented by changing the route attributes such as reachability.

When a router distributes or receives routing information, it may need to implement some policies to filter the routing information, so as to receive or distribute only the routing information meeting given conditions. A routing protocol (RIP, for example) may need to import the routing information discovered by other protocols to enrich its routing knowledge. While importing routing information from another protocol, it possibly only needs to import the routes meeting given conditions and control some attributes of the imported routes to make the routes meet the requirements of this protocol.

For the implementation of a route policy, you need to define a set of matching rules by specifying the characteristics of the routing information to be filtered. You can set the rules based on such attributes as destination address and source address of the information. The matching rules can be set in advance and then used in the routing policies to advertise, receive, and import routes.

Filters

A routing protocol can reference an ACL, IP-prefix, or route policy to filter routing information. The following sections describe these filters.

ACL

You can specify a range of IP addresses or subnets when defining an ACL so as to match the destination network addresses or next-hop addresses in routing information. You can reference an ACL into a route policy to filter routing information.

For ACL configuration, refer to the part discussing ACL.

Route policy

A route policy is used to match some attributes with given routing information and the attributes of the information will be set if the conditions are satisfied.

A route policy can comprise multiple nodes. Each node is a unit for matching test, and the nodes will be matched in ascending order of their node numbers. Each node comprises a set of **if-match** and **apply** clauses. The **if-match** clauses define the matching rules. The matching objects are some attributes of routing information. The relationship among the **if-match** clauses for a node is “AND”. As a result, a matching test against a node is successful only when all the matching conditions specified by the **if-match** clauses in the node are satisfied. The **apply** clauses specify the actions performed after a matching test against the node is successful, and the actions can be the attribute settings of routing information.

There is an OR relationship between different nodes in a route policy. As a result, the system examines the nodes in the route policy in sequence, and once the route matches a node in the route policy, it will pass the matching test of the route policy without entering the test of the next node.

IP Route Policy Configuration Task List

Complete the following tasks to configure an IP route policy:

Task		Remarks
Route Policy Configuration	Defining a Route Policy	Required
	Defining if-match Clauses and apply Clauses	Required

Route Policy Configuration

A route policy is used to match given routing information or some attributes of routing information and change the attributes of the routing information if the conditions are met. The above-mentioned filtering lists can serve as the match conditions:

A route policy can comprise multiple nodes and each node comprises:

- **if-match** clause: Defines matching rules; that is, the filtering conditions that the routing information should satisfy for passing the current route policy. The matching objects are some attributes of the routing information.
- **apply** clause: Specifies actions, which are the configuration commands executed after a route satisfies the filtering conditions specified by the **if-match** clause. Thereby, some attributes of the route can be modified.

Configuration Prerequisites

Before configuring a route policy, perform the following tasks:

- Configuring a filtering list,
- Configuring a routing protocol

Prepare the following data before the configuration:

- Route policy name and node number

- Match conditions
- Route attributes to be changed

Defining a Route Policy

Follow these steps to define a route policy:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Define a route policy and enter the route policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	Required Not defined by default

Note

- The **permit** argument specifies the matching mode for a defined node in the route policy to be in **permit** mode. If a route matches the rules for the node, the **apply** clauses for the node will be executed and the test of the next node will not be taken. If not, however, the route takes the test of the next node.
- The **deny** argument specifies the matching mode for a defined node in the route policy to be in **deny** mode. In this mode, no **apply** clause is executed. If a route satisfies all the **if-match** clauses of the node, no **apply** clause for the node will be executed and the test of the next node will not be taken. If not, however, the route takes the test of the next node.
- If multiple nodes are defined in a route policy, at least one of them should be in **permit** mode. When a route policy is applied to filtering routing information, if a piece of routing information does not match any node, the routing information will be denied by the route policy. If all the nodes in the route policy are in **deny** mode, all routing information will be denied by the route policy.

Defining if-match Clauses and apply Clauses

Follow these steps to define if-match clauses and apply clauses:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter the route-policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	Required
Define a rule to match the IP address of routing information	**if-match acl** *acl-number*	Optional By default, no matching is performed on the address of routing information.
Define a rule to match the cost of routes	**if-match cost** *value*	Optional By default, no matching is performed against the cost of routes.
Define a rule to match the next-hop interface of routing information	**if-match interface** *interface-type interface-number*	Optional By default, no matching is performed on the next-hop interface of routing information.

To do...	Use the command...	Remarks
Define a rule to match the next-hop address of routing information	**if-match ip next-hop acl** *acl-number*	Optional By default, no matching is performed on the next-hop address of routing information.
Apply a cost to routes satisfying matching rules	**apply cost** *value*	Optional By default, no cost is applied to routes satisfying matching rules.

Note

- A route policy comprises multiple nodes. There is an OR relationship between the nodes in a route policy. As a result, the system examines the nodes in sequence, and once the route matches a node in the route policy, it will pass the matching test of the route policy without entering the test of the next node.
- During the matching, there is an AND relationship between the **if-match** clauses for a route policy node. That is, a matching test against a node is successful only when all the matching conditions specified by the **if-match** clauses in the node are satisfied.
- If no **if-match** clauses are specified, all the routes will filter through the node.
- A node can comprise no **if-match** clause or multiple **if-match** clauses.
- Each node comprises a set of **if-match** and **apply** clauses. **if-match** clauses define matching rules. **apply** clauses specify the actions performed after a matching test against the node is successful, and the actions can be the attribute settings of routing information.

Displaying and Maintaining IP Route Policy

To do...	Use the command...	Remarks
Display route policy information	**display route-policy** [*route-policy-name*]	Available in any view

IP Route Policy Configuration Example

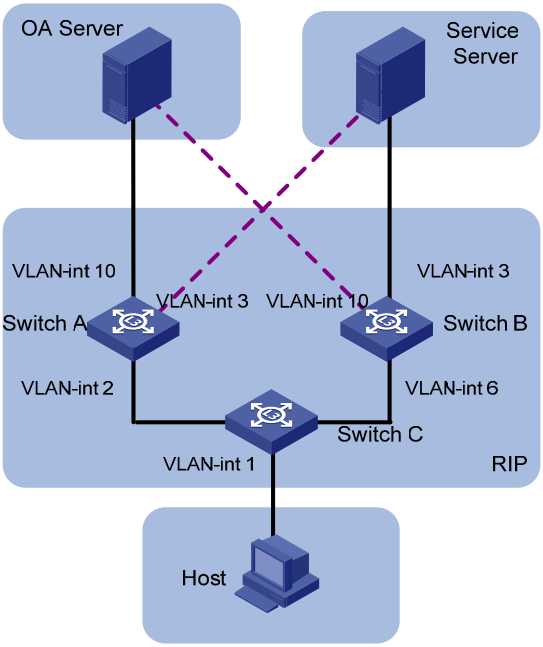
Controlling RIP Packet Cost to Implement Dynamic Route Backup

Network requirements

The required speed of convergence in the small network of a company is not high. The network provides two services. Main and backup links are provided for each service for the purpose of reliability. The main link of one service serves as the backup link of the other. The two services are distinguished by IP addresses. If a fault occurs to the main link of one service, dynamic backup can prevent service interruption.

According to the network requirements, the network topology is designed as shown in Figure 4-1.

Figure 4-1 Network diagram



Device	Interface	IP address
Switch A	Vlan-int 2	2.2.2.1/8
	Vlan-int 3	3.3.3.254/8
	Vlan-int 10	1.1.1.254/8
Switch B	Vlan-int 3	3.3.3.253/8
	Vlan-int 6	6.6.6.5/8
	Vlan-int 10	1.1.1.253/8
Switch C	Vlan-int 1	192.168.0.39/24
	Vlan-int 2	2.2.2.2/8
	Vlan-int 6	6.6.6.6/8
OA Server		1.1.1.1/32
Service Server		3.3.3.3/32
Host		192.168.0.9/24

Configuration considerations

- According to the network requirements, select RIP.
- For the OA server, the main link is between Switch A and Switch C, while the backup link is between Switch B and Switch C.
- For the service server, the main link is between Switch B and Switch C, while the backup link is between Switch A and Switch C.
- Apply a route policy to control the cost of routes received by Switch C to provide main and backup links for the services of the OA server and service server.

Configuration procedure

1) Configure Switch A.

Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

Configure RIP.

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip] network 1.0.0.0
```

```
[SwitchA-rip] network 2.0.0.0
[SwitchA-rip] network 3.0.0.0
```

2) Configure Switch B.

Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

Configure RIP.

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip] network 1.0.0.0
[SwitchB-rip] network 3.0.0.0
[SwitchB-rip] network 6.0.0.0
```

3) Configure Switch C.

Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

Define IP-prefix 1 containing the IP address prefix 1.0.0.0/8, and IP-prefix 2 containing the IP address prefix 3.0.0.0/8.

```
<SwitchC> system-view
[SwitchC] acl number 2000
[SwitchC-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchC-acl-basic-2000] quit
[SwitchC] acl number 2001
[SwitchC-acl-basic-2000] rule permit source 3.0.0.0 0.255.255.255
[SwitchC-acl-basic-2000] quit
```

Create a route policy named **in** and node 10 with the matching mode being **permit**. Define if-match clauses. Apply the cost 5 to routes matching the outgoing interface VLAN-interface 2 and ACL 2000.

```
[SwitchC] route-policy in permit node 10
[SwitchC-route-policy] if-match interface Vlan-interface2
[SwitchC-route-policy] if-match acl 2000
[SwitchC-route-policy] apply cost 5
[SwitchC-route-policy] quit
```

Create node 20 with the matching mode being **permit** in the route policy. Define if-match clauses. Apply the cost 6 to routes matching the outgoing interface VLAN-interface 2 and ACL 2001.

```
[SwitchC] route-policy in permit node 20
[SwitchC-route-policy] if-match interface Vlan-interface2
[SwitchC-route-policy] if-match acl 2001
[SwitchC-route-policy] apply cost 6
[SwitchC-route-policy] quit
```

Create node 30 with the matching mode being **permit** in the route policy. Define if-match clauses. Apply the cost 6 to routes matching the outgoing interface VLAN-interface 6 and ACL 2000.

```
[SwitchC] route-policy in permit node 30
[SwitchC-route-policy] if-match interface Vlan-interface6
[SwitchC-route-policy] if-match acl 2000
[SwitchC-route-policy] apply cost 6
[SwitchC-route-policy] quit
```

Create node 40 with the matching mode being **permit** in the route policy. Define if-match clauses. Apply the cost 5 to routes matching the outgoing interface VLAN-interface 6 and ACL 2001.

```
[SwitchC] route-policy in permit node 40
[SwitchC-route-policy] if-match interface Vlan-interface6
[SwitchC-route-policy] if-match acl 2001
[SwitchC-route-policy] apply cost 5
[SwitchC-route-policy] quit
```

Create node 50 with the matching mode being **permit**, to allow all routing information to pass.

```
[SwitchC] route-policy in permit node 50
[SwitchC-route-policy] quit
```

Configure RIP and apply the route policy **in** to the incoming routing information.

```
[SwitchC] rip
[SwitchC-rip] network 1.0.0.0
[SwitchC-rip] network 3.0.0.0
[SwitchC-rip] network 6.0.0.0
[SwitchC-rip] filter-policy route-policy in import
```

Configuration verification

1) Display data forwarding paths when the main link of the OA server between Switch A and Switch C works normally.

```
<SwitchC> display ip routing-table
 Routing Table: public net
Destination/Mask    Protocol   Pre  Cost      Nexthop         Interface
1.0.0.0/8           RIP        100  5         2.2.2.1         Vlan-interface2
2.0.0.0/8           DIRECT     0    0         2.2.2.2         Vlan-interface2
2.2.2.2/32          DIRECT     0    0         127.0.0.1       InLoopBack0
3.0.0.0/8           RIP        100  5         6.6.6.5         Vlan-interface6
6.0.0.0/8           DIRECT     0    0         6.6.6.6         Vlan-interface6
6.6.6.6/32          DIRECT     0    0         127.0.0.1       InLoopBack0
127.0.0.0/8         DIRECT     0    0         127.0.0.1       InLoopBack0
127.0.0.1/32        DIRECT     0    0         127.0.0.1       InLoopBack0
192.168.0.0/24      DIRECT     0    0         192.168.0.39    Vlan-interface1
192.168.0.39/32     DIRECT     0    0         127.0.0.1       InLoopBack0
```

2) Display data forwarding paths when the main link of the OA server between Switch A and Switch C is down.

```
<SwitchC> display ip routing-table
 Routing Table: public net
Destination/Mask    Protocol   Pre  Cost      Nexthop         Interface
1.0.0.0/8           RIP        100  6         6.6.6.5         Vlan-interface2
3.0.0.0/8           RIP        100  5         6.6.6.5         Vlan-interface6
6.0.0.0/8           DIRECT     0    0         6.6.6.6         Vlan-interface6
6.6.6.6/32          DIRECT     0    0         127.0.0.1       InLoopBack0
127.0.0.0/8         DIRECT     0    0         127.0.0.1       InLoopBack0
127.0.0.1/32        DIRECT     0    0         127.0.0.1       InLoopBack0
192.168.0.0/24      DIRECT     0    0         192.168.0.39    Vlan-interface1
192.168.0.39/32     DIRECT     0    0         127.0.0.1       InLoopBack0
```

Precautions

1) When you configure the **apply cost** command in a route policy:
- The new cost should be greater than the original one to prevent RIP from generating routing loop in the case that a loop exists in the topology.
- The cost will become 16 if you try to set it to a value greater than 16.
- The cost will become the original one if you try to set it to 0.
- The cost will still be 16 if you try to set it to 16.

2) Using the **if-match interface** command will match the routes whose outgoing interface to the next hop is the specified interface.
3) You are recommended to configure a node to match all routes not passing the preceding nodes in a route policy.
4) If the cost of a received RIP route is equal to 16, the cost specified by the **apply cost** command in a route policy will not be applied to the route, that is, the cost of the route is equal to 16.
5) Using the **filter-policy** command does not filter redistributed routes.

Troubleshooting IP Route Policy

Symptom

The route policy cannot filter routing information correctly when the routing protocol runs normally.

Analysis

The route policy cannot filter routing information correctly in the following two cases:

- All nodes in the route policy are in the **deny** mode.
- All entries in the IP-prefix list are in the **deny** mode.

Solution

1) Use the **display ip ip-prefix** command to display the configuration of the IP-prefix list.
2) Use the **display route-policy** command to display the configuration of the route policy.

Table of Contents

1 UDP Helper Configuration ····· 1-1
Introduction to UDP Helper ····· 1-1
Configuring UDP Helper ····· 1-2
Displaying and Maintaining UDP Helper ····· 1-3
UDP Helper Configuration Example ····· 1-3
Cross-Network Computer Search Through UDP Helper ····· 1-3

1 UDP Helper Configuration

When configuring UDP helper, go to these sections for information you are interested in:

- Introduction to UDP Helper
- Configuring UDP Helper
- Displaying and Maintaining UDP Helper
- UDP Helper Configuration Example

Introduction to UDP Helper

Sometimes, a host needs to forward broadcasts to obtain network configuration information or request the names of other devices on the network. However, if the server or the device to be requested is located in another broadcast domain, the host cannot obtain such information through broadcast.

To solve this problem, the unified switches provide the UDP Helper function to relay specified UDP packets. In other words, UDP Helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified destination server.

With UDP Helper enabled, the device decides whether to forward a received UDP broadcast packet according to the UDP destination port number of the packet.

- If the destination port number of the packet matches the one pre-configured on the device, the device modifies the destination IP address in the IP header and then sends the packet to the specified destination server.
- Otherwise, the device sends the packet to the upper layer protocol for processing.

Note

Relay forwarding of BOOTP/DHCP broadcast packets is implemented by the DHCP relay function using UDP ports 67 and 68, so these two ports cannot be configured as UDP Helper relay ports.

By default, with UDP Helper enabled, the device forwards broadcast packets with the six UDP destination port numbers listed in Table 1-1.

Table 1-1 List of default UDP ports

Protocol	UDP port number
DNS (Domain Name System)	53
NetBIOS-DS (NetBIOS Datagram Service)	138
NetBIOS-NS (NetBIOS Name Service)	137
TACACS (Terminal Access Controller Access Control System)	49
TFTP (Trivial File Transfer Protocol)	69

Protocol	UDP port number
Time Service	37

Configuring UDP Helper

Follow these steps to configure UDP Helper:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable UDP Helper	**udp-helper enable**	Required Disabled by default.
Specify a UDP port number	**udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }	Optional By default, the device enabled with UDP Helper forwards the broadcast packets containing any of the six port numbers 53, 138, 137, 49, 69 and 37.
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Specify the destination server to which the UDP packets are to be forwarded	**udp-helper server** *ip-address*	Required No destination server is specified by default.

Note

- You need to enable UDP Helper before specifying any UDP port to match UDP broadcasts; otherwise, the configuration fails. When the UDP helper function is disabled, all configured UDP ports are disabled, including the default ports.
- The **dns**, **netbios-ds**, **netbios-ns**, **tacacs**, **tftp**, and **time** keywords correspond to the six default ports. You can configure the default ports by specifying port numbers or the corresponding parameters. For example, **udp-helper port** 53 and **udp-helper port dns** specify the same port.
- You can specify up to 20 destination server addresses on a VLAN interface.
- If UDP Helper is enabled after a destination server is configured for a VLAN interface, the broadcasts from interfaces belonging to the VLAN and having a matching UDP port will be unicast to the destination server.

Displaying and Maintaining UDP Helper

To do…	Use the command…	Remarks
Display the UDP broadcast relay forwarding information of a specified VLAN interface on the device	**display udp-helper server** [**interface vlan-interface** *vlan-id*]	Available in any view
Clear statistics about packets forwarded by UDP Helper	**reset udp-helper packet**	Available in user view

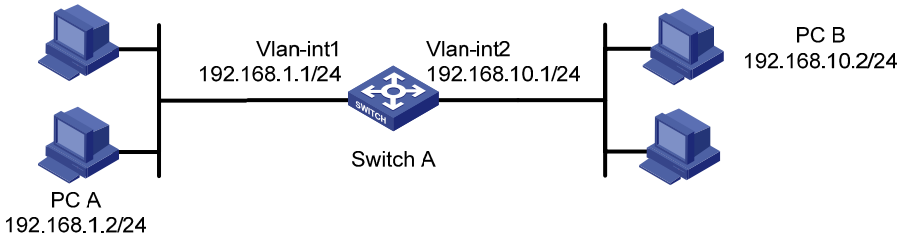
UDP Helper Configuration Example

Cross-Network Computer Search Through UDP Helper

Network requirements

As shown in Figure 1-1, PC A resides on network segment 192.168.1.0/24 and PC B on 192.168.10.0/24; they are connected through Switch A and are routable to each other. It is required to configure UDP Helper on Switch A, so that PC A can find PC B through computer search. (Broadcasts with UDP port 137 are used for searching.)

Figure 1-1 Network diagram for UDP Helper configuration



Configuration procedure

Enable UDP Helper on Switch A.

```
<SwitchA> system-view
[SwitchA] udp-helper enable
```

Configure Switch A to forward broadcasts containing the destination UDP port number 137. (By default, the device enabled with UDP Helper forwards the broadcasts containing the destination UDP port number 137.)

```
[SwitchA] udp-helper port 137
```

Specify the destination server IP address on Vlan-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] udp-helper server 192.168.10.2
```

Table of Contents

Appendix A Acronyms **A-1**

Appendix A Acronyms

A	
AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
ACL	Access Control List
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Border Router
B	
BDR	Backup Designated Router
C	
CAR	Committed Access Rate
CLI	Command Line Interface
CoS	Class of Service
D	
DDM	Distributed Device Management
DLA	Distributed Link Aggregation
DRR	Distributed Resilient Routing
DHCP	Dynamic Host Configuration Protocol
DR	Designated Router
D-V	Distance Vector Routing Algorithm
E	
EGP	Exterior Gateway Protocol
F	
FTP	File Transfer Protocol
G	
GE	Gigabit Ethernet
I	
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
IRF	Intelligent Resilient Framework

L	
LSA	Link State Advertisement
LSDB	Link State DataBase
M	
MAC	Medium Access Control
MIB	Management Information Base
N	
NBMA	Non Broadcast MultiAccess
NIC	Network Information Center
NMS	Network Management System
NVRAM	Nonvolatile RAM
P	
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
Q	
QoS	Quality of Service
R	
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
S	
SNMP	Simple Network Management Protocol
SP	Strict Priority
STP	Spanning Tree Protocol
T	
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
ToS	Type of Service
TTL	Time To Live
U	
UDP	User Datagram Protocol
V	
VLAN	Virtual LAN
VOD	Video On Demand
W	
WRR	Weighted Round Robin